IJNS
International Journal of Network Security

ISSN 1816-353X (Print)
ISSN 1816-3548 (Online)

Vol. 25, No. 4 (July 2023)

INTERNATIONAL JOURNAL OF NETWORK SECURITY

PUBLISHING OFFICE

Min-Shiang Hwang
Department of Computer Science & Information Engineering, Asia University, Taichung 41354, Taiwan, R.O.C.
Email: mshwang@asia.edu.tw

International Journal of Network Security is published both in traditional paper form (ISSN 1816-353X) and in Internet (ISSN 1816-3548) at http://ijns.jalaxy.com.tw

PUBLISHER: Candy C. H. Lin

Volume: 25, No: 4 (July 1, 2023)

International Journal of Network Security

Security Situation Assessment Method of Industrial Control System Network Based on Sine-SSA-BP

Peng-Shou Xie, Hong Wang, Jia-Lu Wang, Xiao-Ye Li, Yin-Chang Pan, and Tao Feng
(Corresponding author: Hong Wang)

School of Computer and Communications, Lanzhou University of Technology
No. 36 Peng Jia-ping Road, Lanzhou, Gansu 730050, China
Email: corresponding_authors@email.address
(Received July 29, 2022; Revised and Accepted May 28, 2023; First Online June 24, 2023)

Abstract

The existing industrial control system network security situation assessment is mainly faced with an incomplete index system and low accuracy of assessment methods. In this paper, to address the above problems, by analyzing the characteristics of the operational status of this network, we design a security situation assessment indexes system and security situation classification scheme for industrial control system network containing factors such as attack impact, vulnerability threat, asset, defense measures; and propose a security situation assessment method for industrial control system network based on Sine-SSA-BP. The current network security situation is comprehensively demonstrated through the classified security situation and quantitative assessment results. The method uses Sine optimized SSA algorithm to solve the problems of low training efficiency and low evaluation accuracy of the SSA-BP network. The experimental results show that the proposed method can comprehensively evaluate network security situations, and the evaluation accuracy is higher than the existing methods.

Keywords: BP; Industrial control system network; Situation assessment; Sine; SSA

1 Introduction

1.1 Related Works

With "Industry 4.0" and the Internet of things bringing the third wave of development of the global information industry, the deep integration of industrial control systems and the Internet has been widely used in modern industrial fields such as electric power, water conservancy, metallurgy, petrochemicals, aerospace, etc [4, 6]; It has developed towards digitalization, networking, and intelligence, making it exposed to more threats and attacks [9]. For example, the natural gas pipeline network in the UK was attacked in August 2019, resulting in the shutdown of the gas power station, as well as the Shamoon virus, Petya ransomware virus, "Flame" virus, Ukraine power grid virus incidents, etc. It has had a serious impact on national security, economic development, ent, and social stability. Traditional network security defense technology: access control, firewall, traffic detection, intrusion detection. They only passively defend a certain area of themselves, and the lack of correlation between various defensive measures makes it difficult to form an organic integral defense [11,16]. Accurate and efficient evaluation of target network security status is of great significance to the stable and safe operation of the network [18, 22]. Network security situational awareness technology is one of the most effective active defense technologies to assess network security threats [7,21]. It can effectively monitor and control the overall operation of the industrial control system network by using situational awareness technology, to ensure the safe operation of the network.

At present, the most widely used model frameworks in the field of situational awareness research are the Endsley model, Tim Bass model, and JDL (Joint Directors of Laboratories) model [14, 19]. However there are inherent differences between Industrial Control System Network and Traditional Internet, and Traditional Internet security situation assessment indicators cannot be fully applied to Industrial Control System Network.

Therefore, it is necessary to comprehensively understand and master the security status of the industrial control system network based on the traditional network security situational awareness, combined with the characteristics of the industrial control system network and the analysis of the existing security problems.

Tao *et al.* [13] proposed a network domain security situation assessment method based on SAE-BPNN for the high-dimensionality of input data, the complexity of model construction, and the non-objectiveness of the index weight. This method extracts and normalizes the

index data in the network domain, which reduces the data storage cost and improves computational efficiency. Zhang *et al.* [23] described the network situation by obtaining the probability and impact of each attack against the problem of only attacking and normal labels. Made the prediction results more in line with the actual situation of the network. The model uses the DT algorithm and LSTM network to study the time series problem of network security situation assessment and quantitatively evaluate the network situation. Dong *et al.* [3] aimed at the problems of the high complexity of existing network security situation assessment methods and poor effect in the big data environment. An assessment model based on SimHash in a big data environment is proposed. The model divides the large-scale network into multiple modules and obtains the security data of the internal nodes of the module. The node security situation, module security situation, and network security situation are quantified in turn. Wang *et al.* [15] aimed at the impact of vulnerabilities on specific networks, considering the availability of vulnerabilities, the impact of vulnerabilities on network components, and the importance of vulnerability components, a vulnerability risk assessment method based on heterogeneous information networks is proposed.

Cai *et al.* [2] the weight analysis method used to construct the hierarchical graph of the situation assessment model, and the security situation of the network host node is calculated from the aspects of log audit and the network performance. The theoretical security threat is obtained through the correlation analysis of multiple logs, and then the security situation of the node is corrected in real-time according to the network performance information. Finally, the comprehensive network security situation value is calculated by the importance weight of the network node. Zhao *et al.* [24] Situational awareness indicators are established from three aspects: vulnerability, threat, and asset importance; PCA clustering is used to preprocess the alarm information and delete the useless information, to establish the fusion rule of multi-source alarm data and apply DS theory to quantify the situation indicators to achieve high-precision situation assessment. Liao *et al.* [10] an improved Hidden Markov Model is proposed, which extends the five-tuple in the traditional hidden Markov model to a seven-tuple to form a new HMMP model, and adds two parameters of network defense efficiency and risk loss vector so that the model can describe the network security situation more comprehensively. Tang *et al.* [12] proposed an optimized cloud model DDoS attack situation assessment method based on the impact function for the existing network security situation assessment methods that cannot effectively assess DDoS attack situations.

In summary, the existing research provides a series of feasible solutions for network security situation assessment, but there are still some problems. For example, the evaluation accuracy is insufficient, the assessment process is complicated, the indicator rights are determined by experience or subjective opinions of domain experts, and there is little research on the network situation assessment of industrial control systems. In response to these problems, this paper proposes a Sine-SSA-BP neural network security situation assessment method based on the characteristics of industrial control system networks, which can effectively deal with complex and diverse industrial control system network attacks.

1.2 Organization

The remainder of this paper is organized as follows. Section 2 introduces the industrial control system network security situation assessment index system and security situation classification scheme. Section 3 introduces the security situation assessment method based on the Sine-SSA-BP network. Section 4, the proposed evaluation indexes and assessment methods is experimentally verified, and the performance is compared with the existing methods. Section 5 concludes the presented work and raises several issues for future work.

2 Industrial Control System Network Security Situation Assessment Index System

The industrial control system network security situation assessment index system is an important link in the situation assessment, and the construction of a reasonable network security situation assessment index system can lay the foundation for the network security situation assessment.The expression of network security situational awareness is: $SV = F(X) = f1(x1)\&f2(x2)\&\ldots\&gn(xn)$, SV is the assessment result, F is the fusion algorithm,$x1, x2, ..., xn$ is the specific analysis index;$f1, f2, ..., fn$ is the performance of various fusion algorithms, and & is the integration process of the assessment system.

2.1 Security Situation Assessment Indicators

To realize the accurate assessment of the network security situation of the industrial control system, and at the same time facilitate the description of the evaluation results, given the complexity and heterogeneity of the operating data of the industrial control system network and the relationship between various impact indicators, combined with the construction principles of situation assessment index system. The situation assessment of the network security is carried out through the attack impact $F1$,the vulnerability threat $F2$, the asset $F3$ and the defense measure $F4$, to obtain the current network situation value SV of the system.$SV = f(F1, F2, F3, F4)$.The higher the situation value represents the overall situation of the system network is not safe, and need to take high-intensity defense measures; the lower the situation value represents

the overall situation of the system network is safer.

1) Attack Impact F1 (Parameter 1, Parameter 2, Parameter 3)

Parameter 1: Attack Quantity Factor: The total number of attacks captured by security devices over a certain period of time; denoted as N_A.

Parameter 2: Attack Frequency Factor: The attack frequency of the same type of attack in a certain period of time; denoted as$B_A(t)$ (i represents a different type of attack).

Parameter 3: Attack Threat Factor: The impact of different attack types on the safe operation of the industrial control system network; denoted as $X_{Ai}(t)$ (i represents a different type of attack).

2) Vulnerability Threat F2 (Parameter 4, Parameter 5, Parameter 6)

Parameter 4: Vulnerability Quantity Factor: The total number of vulnerabilities scanned in a certain period of time; denoted as N_V.

Parameter 5: Vulnerability Frequency Factor: The frequency of various types of vulnerabilities used in a certain period of time; denoted as $B_V(t)$ (i represents a different type of vulnerability).

Parameter 6: Vulnerability Threat Factor: The impact of different vulnerability types on the network security operation of the industrial control system; denoted as $X_{V_i}(t)$ (i represents a different type of vulnerability).

3) Asset F3 (Asset importance, Confidentiality, Integrity, Availability)

Parameter 7: Asset importance ASI: the value of different assets and assets can be divided into hardware assets, software assets, and information assets; according to the different requirements of the assets on each security attribute, the value of the assets is measured from the confidentiality, integrity, and availability, and can be obtained by Equation (1) weighted calculation; Asset can therefore be assigned to five different levels and the higher the level is, the more important the asset is: 5 (very high), 4 (high), 3 (medium), 2 (low), 1 (very low):

$$\mathrm{ASI_i} = \lg\left(\frac{\mathrm{w_1}10^{\mathrm{C_i}} + \mathrm{w_2}10^{\mathrm{I_i}} + \mathrm{w_3}10^{\mathrm{A_i}}}{3}\right) \quad (1)$$

Among them: i represents the type i assets,w_1 ,w_2 and w_3 are the normalized weights of C, I and A respectively;C_i ,I_i andA_i are the influence degrees of C, I and A for each asset type, respectively; according to no influence, low influence, and high influence are divided into three levels, respectively assigned value : 0, 0.5, 1.

4) Defense measure F4 (basic operation index)

Defense measure refers to the existing encryption technology, firewall technology, intrusion detection technology, and network security protocol in the industrial control system network; in this paper, the defense measures are divided according to the ratio of the number of successful defense attacks to the total number of mountain attacks, which can be divided into three levels, namely, high, medium and low, and the assignments are corresponding to (3, 2, 1). Calculated by Equation (2).

$$\mathrm{F4} = \frac{1}{\mathrm{Defense}} \quad (2)$$

2.2 Quantification of Security Situation Assessment Indicators

1) Quantification of attack and vulnerability threat factors

This paper combines the theory of weight coefficient generation [20] and attack severity level and vulnerability threat level to calculate the size of the attack threat factor and the vulnerability threat intensity of each attack type.

Divide n types of attacks and vulnerabilities into C types of attack severity levels and vulnerability severity levels from high to low. The attack threat factor of the ith attack type is X_{A_i}, and the vulnerability threat factor of the ith vulnerability type is X_{V_i} calculated by Equation (3), which C_i represents the attack severity of the ith attack type and the vulnerability severity of the ith vulnerability type.

$$\mathrm{X_i} = \begin{cases} \frac{1}{2} + \frac{\sqrt{-2\ln\frac{2\mathrm{C_i}}{\mathrm{n}}}}{6}, & 1 \leqslant \mathrm{C_i} < \frac{\mathrm{n}}{2} \\ \frac{1}{2}, & \mathrm{C_i} = \frac{\mathrm{n}}{2} \\ \frac{1}{2} - \frac{\sqrt{-2\ln\left[2-\frac{2\mathrm{C_i}}{\mathrm{n}}\right]}}{6}, & \frac{\mathrm{n}}{2} < \mathrm{C_i} < \mathrm{n} \end{cases} \quad (3)$$

2) The severity level of each attack and the size of the attack threat factors. Shown in Table 1

Table 1: Various types of attacks

Attack level	Attack type	Xi
1	MPCI	0.789
1	MFCI	0.789
2	MSCI 3	0.712
3	CMRI 2	0.650
4	NMRI 1	0.581
5	Recon	0.419
6	DOS	0.288

3) The severity level of each vulnerability and the size of vulnerability threat factors. Shown in Table 2.

Table 2: Various types of vulnerabilities

Vulnerability level	Vulnerability type	Xi
1	Generic	0.789
2	Exploits	0.712
2	Fuzzers	0.712
3	Analysis	0.650
4	Backdoor	0.581
5	Shellcode	0.419
6	Worms	0.288

4) Quantification of attack impact
$F_A(t)$denotes the attack impact index of a certain attack type in the t period. For each attack, the strength calculation formula of the index factor at t time is as follows Equation (4).

$$\begin{aligned} \mathrm{F_{Ai}(t)} &= \mathrm{f\,(N, B_{Ai}(t), X_{Ai}(t))} \\ &= \sum_{1}^{\mathrm{n}} \frac{\mathrm{B_{Ai}(t)}}{\mathrm{N}} \times 10^{\mathrm{x_{Ai}(t)}} \end{aligned} \tag{4}$$

5) Quantification of vulnerability impact
$F_V(t)$represents the threat impact index of a vulnerability type in the t period. For each vulnerabiclity, the strength calculation formula of the index factor at t time is as follows Equation (5).

$$\begin{aligned} \mathrm{F_{Vi}(t)} &= \mathrm{f\,(N, B_{Vi}(t), X_{Vi_1}(t))} \\ &= \sum_{1}^{\mathrm{n}} \frac{B_{\mathrm{v_1}}(\mathrm{t})}{\mathrm{N}} \times 10^{\mathrm{X_V(t)}} \end{aligned} \tag{5}$$

2.3 Classification of Security Situation Assessment

Through the construction and quantification of the safety situation assessment index, combined with the safety operation status of the industrial control system network, according to the national emergency plan, combined with the characteristics of network hazards, five kinds of threat evaluation indexes are given, which are divided into five levels: ultra-high risk, severe risk, moderate risk, mild risk, and safety. At the same time, to facilitate the intuitive analysis of the results of the network security situation assessment, the 0—1 numerical value is used to quantitatively represent each security level, as shown in Table 3.

3 Security Situation Assessment Method of Industrial Control System Network Based on Sine-SSA-BP

BP neural network can solve most practical engineering problems, but the model has certain limitations. Firstly, it is easy to fall into the local optimal solution and cannot obtain the global optimal solution. Secondly, the initial network model requires a random small weight coefficient, which makes the model not repeatable. To solve the above problems, this paper studies and optimizes the BP neural network of the sparrow search algorithm based on Sine mapping.

3.1 SSA Algorithm

SSA [17] is a new swarm intelligence optimization algorithm proposed by Xue J in 2020. In this algorithm, individuals can be divided into Discoverer, Follower, and Vigilante. Compared with the traditional algorithm, the structure of the sparrow search algorithm is simple, easy to implement, has fewer control parameters, and does not rely on gradient information.

1) Set n sparrows in the population, then the population composed of all individuals can be expressed as Equation (6).

$$\mathrm{X} = \begin{bmatrix} \mathrm{x_{1,1}} & \mathrm{x_{1,2}} & \cdots & \cdots & \mathrm{x_{1,\ d}} \\ \mathrm{x_{2,1}} & \mathrm{x_{2,2}} & \cdots & \cdots & \mathrm{x_{2,\ d}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \mathrm{x_{n,1}} & \mathrm{x_{n,2}} & \cdots & \cdots & \mathrm{x_{n,d}} \end{bmatrix} \tag{6}$$

Among them, d(dim) represents the dimension of the problem to be optimized, and n represents the number of sparrow populations.

2) The location update for The Discoverer is as follows Equation (7)

$$x_{i,j}^{t+1} = \begin{cases} x_{i,j}^{t} \cdot \exp\left(\frac{-1}{a \times xter\max}\right), & R_2 < \mathrm{ST} \\ x_{i,j}^{t} + Q \cdot L, & R_2 \geq \mathrm{ST} \end{cases} \tag{7}$$

Among them, t represents the number of iterations,$x_{i,j}^{t}$ represents the position information of the first sparrow population in the j-dimensional, itermax represents the maximum number of iterations,a represents the random number of 0 to 1, Q represents a random number obeying normal distribution, L is a $1 * d$ matrix with all elements of 1, $R2$: warning value, ST: security value.

3) The Follower location update as follows Equation (8)

$$x_{i,j}^{t+1} = \begin{cases} Q \cdot \exp\left(\frac{x_{\mathrm{worst}}^{t} - x_{i,j}^{t}}{\mathrm{i}^2}\right), & i > \frac{n}{2} \\ x_{P}^{t+1} + \left|x_{i,j}^{t} - x_{P}^{t+1}\right| \cdot A^{+} \cdot L, & i \leq \frac{n}{2} \end{cases} \tag{8}$$

Among them, x_{worst}^{t} represents the current global worst position, A^{+} represents the $1 * d$ matrix whose elements are randomly assigned to 1 or -1, and x_{P}^{t+1} represents the optimal position found by the current discoverer.

4) The Vigilante position update is as follows Equation (9)

$$\mathrm{x_{i,j}^{t+1}} = \begin{cases} \mathrm{x_{best}^{t}} + \beta \cdot \left|\mathrm{x_{i,j}^{t}} - \mathrm{x_{best}^{t}}\right|, & \mathrm{f_i} \neq \mathrm{f_g} \\ \mathrm{x_{best}^{t}} + \mathrm{k} \cdot \left(\frac{\mathrm{x_{i,j}^{t}} - \mathrm{x_{best}}}{|\mathrm{f_i} - \mathrm{f_w}| + \varepsilon}\right), & \mathrm{f_i} = \mathrm{f_g} \end{cases} \tag{9}$$

Table 3: Safety Classification

Safety index	Safety level	Network status
0.00-0.15	Safe	Normal operation
0.15-0.35	Mild hazard	Slight impact
0.35-0.65	Moderate risk	Greater impact
0.65-0.85	Severe hazard	Serious impact
0.85-1.00	Ultra-high hazard	Serious security incident

Among them, x_{best}^t represents the current global optimal position, f_i represents the fitness value of the current sparrow individual, f_g represents the global best fitness value, and f_w represents the global worst fitness value.

3.2 Sine Optimized SSA Algorithm

Chaotic variables have random characteristics, which can be used to increase the population diversity of the algorithm, improve the ability of the algorithm to select the local optimum, and improve the global search ability of the algorithm in the search optimization problem. The SSA algorithm has the defects of easily falling into local optimum, slow convergence speed, and low convergence accuracy. Therefore, this paper uses the chaotic operator Sine to optimize SSA.

The calculation method of Sine mapping function is shown in Equation (10).

$$x_{k+1} = \frac{a}{4}\sin\left(\pi x_k\right), a \in (0, 4] \tag{10}$$

1) Initialize SSA population n and variable dimension dim;

2) The value of assignment parameter$a$, satisfies the interval range $(0, 4]$;

3) Using the Sine mapping function to generate chaotic sequence length n, namely the number of populations;

4) Using the Sine mapping function to generate a new sequence of dim, and meet the specified range;

5) The generated population n and the variable dimension dim are taken as the initial parameters of SSA;

3.3 Sine-SSA-BP Assessment Method Implementation Steps

1) Original data input. Enter attacks, vulnerabilities, and other data;

2) Data preprocessing. The original data are normalized to $[0, 1]$ to solve the problems of non-convergence and slow convergence caused by singular sample data;

3) Determine BP neural network topology. The indicators in the situation assessment system are used as the input of the BP neural network to determine the BP neural network topology, where the number of neurons in the input layer is $n = 16$, and the model has only one output variable, so the number of neurons in the output layer is $q = 1$. The number of hidden layer neurons is $\mathrm{m} = \sqrt{\mathrm{n} + \mathrm{l}} + \mathrm{a}$, and the value is a constant between 1 and 10. By comprehensively examining the network accuracy and generalization ability, the optimal results can be obtained according to the trial-and-error method. Finally, the number of hidden nodes is determined to be 12, so the network topology is set to be 16–12–1;

4) Parameter initialization. The sine mapping strategy is used to determine the initial population of SSA, the number of iterations, and the ratio column of predator and adder; determine population size and the maximum number of iterations, and set warning values, and a number of alerts;

5) Define fitness function and calculate individual fitness value. The neural network is trained by using the initial weight threshold, and the sum of the absolute error of the predicted output value and the actual output value is used as the fitness function. The smaller the fitness value is, the smaller the error is. Thus, the current global optimal solution is obtained and the corresponding position is determined;

6) Update the sparrow location. (1) Determine the number of discoverers in the sparrow population and calculate their updated position according to Equation (7); (2) Determine the number of followers in the sparrow population and calculate their updated position according to Equation (8); (3) Determine the number of individuals aware of the danger in the sparrow population, and calculate the position after updating according to Equation (9);

7) Select the global optimal solution. The individual fitness value after the location update is viewed and compared with the current optimal fitness value to compare and select the global optimal solution; otherwise, an iterative calculation is carried out again;

8) The output of the optimal solution as the neural network weights and thresholds;

9) The Sine-SSA optimized BP neural network model is used to evaluate the safety situation of the industrial control system network;

10) Output the situation value of the industrial control system network;

4 Experimental Scheme and Result Analysis

The experimental environment used in this paper is Inter(R) Core(TM)i5-9300H, CPU 2.40GHz, Memory 8GB, GTX1650 4GB video memory. The software environment is Windows 10, MATLAB R2019b, and Python3.6.

The data sets selected in this paper are the Gas Pipeline data set of the natural gas pipeline SCADA system based on the MODBUS communication protocol, and the UNSW-NB 15 data set. The Gas Pipeline dataset contains a total of 214,580 records of Modbus network packets; it contains 4 categories of cyberattacks: Response Injection, Reconnaissance, DOS, and Command Injection [5]. The UNSW-NB 15 dataset contains a training set of 175341 records and a test set of 82332 records, which contain a total of 9 categories of network attacks [1, 8].

4.1 Experimental Description

This paper mainly studies the security situation assessment of industrial control system networks.The existing industrial control system network data set only has attack-type data and does not provide vulnerability threats, asset elements, defense measures, and other related data.There is a single feature problem, which cannot evaluate the security situation of the industrial control system network from multiple perspectives.Therefore, this paper also uses the UNSW-NB 15 datasets and takes the attack in this datasets as a vulnerability threat to the industrial control system network for experiments.For asset elements, this paper uses Equation (1) to assign them after analyzing the experimental environment. System defense measures are divided by the ratio of the number of successful defense attacks to the total number of attacks through the existing security detection and defense equipment in the industrial control system network and assigned by Equation (2) according to the corresponding value of high, medium, and low.

Since the impact of attacks on the network is not only formed by the threat information of the attack itself, but also by the interaction with external attack information and internal vulnerability information of the system; the industrial control system network situation assessment has a strong periodicity. Therefore, the Gas Pipeline and UNSW-NB 15 sample set data are randomly extracted during the evaluation period to simulate attack operations, and the intrusion detection equipment and vulnerability detection equipment are used to obtain attack and vulnerability information.Using python3.6 and MATLAB to simulate the attack operations of four different assessment cycles respectively. Obtain the attack information and vulnerability information in the assessment cycle, count various attack types and vulnerability types in the cycle, and count the attack frequency of various attacks; And using the theory of weight coefficient generation, the threat factors of these attacks and vulnerabilities are calculated.

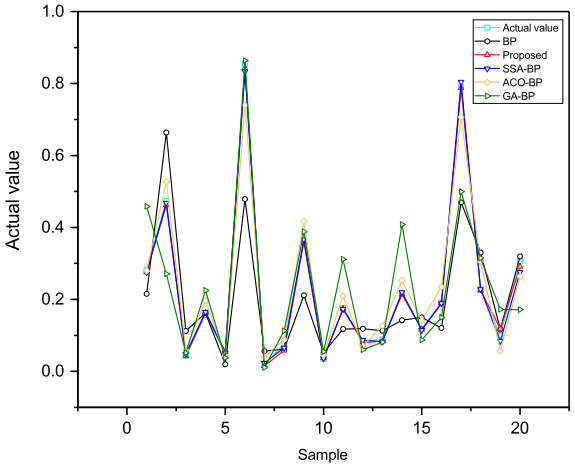


Figure 1: Comparison of Assessment Results

Then, the threat severity of some type of attack on the network security of the system during this period is quantified. After obtaining the index factor of situation assessment, this paper uses the proposed situation assessment method based on Sine-SSA-BP for security situation assessment. The assessment results are classified according to the situation value security level as Table 3. Table 4 shows the evaluation results of some samples randomly selected from the test samples to more intuitively compare the difference between the real situation value and the evaluation results of various methods.

It can be seen from Table 4 that the changing trend of network security situation value evaluated by the four models is roughly the same as that of the real network security situation value, but the situation evaluated by this method is more consistent with the real situation. Combined with Table 3 and Table 4 for detailed analysis. The evaluation results of the BP model have the largest gap with the real situation, for example, the evaluation results of samples 2, 6, 9, 16, and 17 differ from the real results. In sample 6, the true posture value was an ultra-high risk, but the SSA-BP and ACO-BP methods were both assessed as a severe risk; only the posture value derived from the method Sine-SSA-BP in this paper was closest to the true posture value. According to the above analysis, the situation value results obtained by the Sine-SSA-BP method in this paper are more accurate and reliable. To present the evaluation results more clearly and intuitively, this paper draws the evaluation results of the network security situation value of the system as shown in Figure 1. It can be seen from this figure that the situation value

Table 4: Security situation assessment results

Sample	Actual	Level	BP	Level	GA-BP	Level	Proposed	Level	SSA-BP	Level	AOC-BP	Level
1	0.2829	Mild	0.2156	Mild	0.4581	Moder	0.2761	Mild	0.2756	Mild	0.279	Mild
2	0.474	Mode	0.6637	Server	0.271	Mild	0.4624	Moder	0.4686	Moder	0.5275	Moder
3	0.0439	Safe	0.1121	Safe	0.051	Safe	0.0424	Safe	0.0487	Safe	0.06	Safe
4	0.1568	Mild	0.162	Mild	0.2252	Mild	0.1626	Mild	0.165	Mild	0.197	Mild
5	0.0498	Safe	0.0197	Safe	0.0374	Safe	0.0547	Safe	0.0518	Safe	0.0425	Safe
6	0.8541	Ultra	0.4789	Moder	0.8434	Server	0.8532	Ultra	0.834	Server	0.7395	Server
7	0.0178	Safe	0.0563	Safe	0.0106	Safe	0.0151	Safe	0.023	Safe	0.0394	Safe
8	0.0766	Safe	0.0616	Safe	0.0106	Safe	0.0581	Safe	0.0659	Safe	0.0885	Safe
9	0.3643	Mode	0.2111	Mild	0.3878	Moder	0.3596	Moder	0.3671	Moder	0.4172	Moder
10	0.0353	Safe	0.1176	Safe	0.0541	Safe	0.0369	Safe	0.0366	Safe	0.0456	Safe
11	0.1767	Mild	0.3115	Safe	0.3115	Mild	0.174	Mild	0.1735	Mild	0.2099	Mild
12	0.0829	Safe	0.1184	Safe	0.0601	Safe	0.0802	Safe	0.0865	Safe	0.0712	Safe
13	0.0889	Safe	0.113	Safe	0.081	Safe	0.0839	Safe	0.0821	Safe	0.1266	Safe
14	0.2161	Mild	0.142	Safe	0.4077	Mild	0.214	Mild	0.2199	Mild	0.2531	Mild
15	0.1186	Safe	0.1503	Mild	0.0872	Safe	0.1168	Safe	0.1147	Safe	0.1411	Safe
16	0.1915	Mild	0.1202	Safe	0.4581	Safe	0.1893	Mild	0.1891	Mild	0.2349	Mild
17	0.7897	Sever	0.4693	Moder	0.4998	Mild	0.7879	Server	0.8045	Server	0.7059	Server
18	0.2283	Mild	0.33	Mild	0.3146	Mild	0.2248	Mild	0.228	Mild	0.3049	Mild
19	0.0993	Safe	0.1169	Safe	0.1719	Mild	0.1185	Safe	0.084	Safe	0.0569	Safe
20	0.3056	Mild	0.3198	Mild	0.1715	Mild	0.2908	Mild	0.2762	Mild	0.2643	Mild

calculated by this method is closest to the real situation value.

4.2 Experimental Result Analysis

In this paper, MAE, MSE, MAPE, RMSE, and time-consuming are used to evaluate the accuracy and efficiency of the evaluation model, and the performance index calculation formula is as follows. Among them, n is the number of samples; Y_i is the expected output of the test sample of the prediction model, y_i is the actual output.

$$MAE = \frac{1}{n}\sum_{i=1}^{n}|Y_i - y_i| \tag{11}$$

$$\text{MSE} = \frac{1}{n}\sum_{i=1}^{n}(Y_i - y_i)^2 \tag{12}$$

$$\text{RMSE} = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(Y_i - y_i)^2} \tag{13}$$

$$\text{MAPE} = \frac{1}{n}\sqrt{\sum_{i=1}^{n}\left(\frac{Y_i - y_i}{Y_i}\right)^2} \times 100\% \tag{14}$$

In this paper, the samples are divided into four different situation databases: 1500 samples, 500 samples, 200 samples, and 100 samples. The evaluation performance indexes of different methods are calculated through the above performance indexes, as shown in Table 5, Table 6, Table 7, and Table 8.

It can be seen from Table 5, Table 6, Table 7, and Table 8 that the error values of the model BP neural network and the GA-BP model are large and the performance is poor. When the number of samples is small, the MAPE error values reach 47.96% and 34.99%, respectively; the error value of the AOC-BP evaluation method is second, reaching 25.86%. When the number of samples is 100, the MAPE value of the situation assessment method proposed in this paper is 0.6%, 20.43%, 29.56% and 42.52% lower than that of the SSA-BP method, AOC-BP method,GA-BP method and BP method respectively; When the number of samples is 1500, the MAPE value of the situation assessment method proposed in this paper is 0.439%, 1.571%, 2.211% and 4.041% lower than that of SSA-BP method, AOC-BP method, GA-BP method and BP neural network respectively. Compared with other assessment indexes, the error value of the situation assessment method proposed in this paper is the lowest.

In terms of running time, as the number of samples increases, the time of the AOC-BP method also increases rapidly, which has a low efficiency for processing large sample data. Although the proposed method is not optimal but compared the optimal results are almost the same;the calculation time of the situation value does not increase significantly, and it has high processing efficiency; and as the number of samples increases,the smaller the error value, the more accurate the predicted results. Comprehensive analysis shows that the method in this paper has better assessment accuracy and can more accurately evaluate the network security situation. The method proposed in this paper is reliable and feasible.

To present the performance of various network security situation assessment methods more intuitively, this paper draws the evaluation error of the network security situation value of the system as shown in Figure 2. It can be seen from the diagram that the error fluctuation of this method is the gentlest compared with other methods, and has been slightly fluctuating on the 0 axis. The errors of other methods fluctuate greatly. Therefore, the situation

Table 5: Comparison of evaluation performance for 1500 samples

Method	MAE	MSE	RMSE	MAPE	Time
BP	5.8e-03	1.3e-04	0.0112	4.19	960.2
AOC-BP	1.5e-03	5.8e-06	2.4e-03	1.72	832.6
GA-BP	3.4e-03	6.9e-06	3.4e-03	2.36	863.2
SSA-BP	5.2e-04	7.2e-07	8.5e-04	0.588	238.9
Proposed	1.5e-04	1.2e-07	3.4e-04	0.149	287.3

Table 6: Comparison of evaluation performance for 500 samples

Method	MAE	MSE	RMSE	MAPE	Time
BP	0.012	3.1e-04	0.018	10.88	242.3
AOC-BP	7.1e-03	1.0e-04	0.01	5.96	203.2
GA-BP	6.2e-03	2.2e-04	0.014	6.25	222.3
SSA-BP	1.6e-03	3.9e-05	3.3e-03	1.39	210.5
Proposed	1.5e-03	1.1e-05	1.9e-03	1.31	238.3

Table 7: Comparison of evaluation performance for 200 samples

Method	MAE	MSE	RMSE	MAPE	Time
BP	0.052	5.3e-03	0.073	39.15	96.2
AOC-BP	0.024	1.2e-03	0.035	18.49	105.6
GA-BP	0.032	2.1e-03	0.052	22.14	99.6
SSA-BP	7.7e-03	8.9e-05	9.5e-03	6.33	79.7
Proposed	5.8e-03	5.7e-05	7.5e-03	4.29	83.6

Table 8: Comparison of evaluation performance for 100 samples

Method	MAE	MSE	RMSE	MAPE	Time
BP	0.085	0.017	0.13	47.96	77.6
AOC-BP	0.038	2.2e-03	0.047	25.86	76.2
GA-BP	0.0583	0.0079	0.089	34.99	76.8
SSA-BP	7.6e-03	1.1e-04	0.011	6.03	72.7
Proposed	6.3e-03	6.9e-05	8.4e-03	5.43	74.8

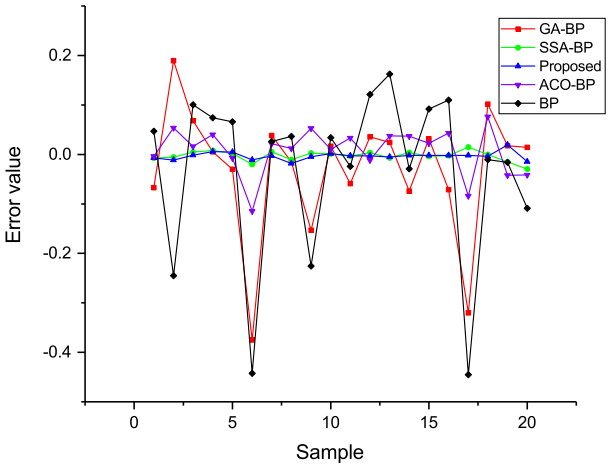


Figure 2: Comparison of error results

assessment method proposed in this paper is more accurate.

5 Conclusions

This paper introduces SSA-BP neural network into the research field of industrial control system network security situation awareness and uses Sine to improve the SSA-BP neural network to form Sine-SSA-BP industrial control system network security situation assessment method. For the selection of indicators in situation assessment, this paper on the attack, vulnerability, assets, and defense four aspects, formed a set of comprehensive responses to the current network situation index factor system. By introducing the weight coefficient generation theory to assign attack threat factor and vulnerability threat factor, the problem that the index weight is determined by subjective experience or subjective opinion of domain experts is avoided. The experimental results show that the improved Sine-SSA-BP method is superior to other assessment methods. The proposed method can evaluate the network security situation more accurately and reliably, which proves the effectiveness of the proposed scheme.

In subsequent studies, on the one hand, it is necessary to study the network security situation prediction of the industrial control system; on the other hand, it is necessary to continuously improve the model to form a complete set of situation assessment-prediction model that can be applied to the industrial control system network.

Acknowledgments

This study was supported by the National Natural Science Foundations of China under Grants No.61862040 and No.61762059. The authors gratefully acknowledge the anonymous reviewers for their valuable comments and suggestions.

References

[1] M. S. Al-Daweri, A. K. A. Zainol, and S. Abdullah, "An analysis of the kdd99 and unsw-nb15 datasets for the intrusion detection system," *Symmetry*, vol. 12, no. 10, p. 1666, 2020.

[2] W. Cai and H. Yao, "Research on information security risk assessment method based on fuzzy rule set," *Wireless Communications and Mobile Computing*, vol. 2021, 2021.

[3] R. H. Dong, C. Shu, and Q. Y. Zhang, "Security situation assessment algorithm for industrial control network nodes based on improved text simhash," *International Journal of Network Security*, vol. 23, no. 6, pp. 973–984, 2021.

[4] Q. Fu, Y. Yao, and C. Sheng, "Interplay between malware epidemics and honeynet potency in industrial control system network," *IEEE Access*, vol. 8, no. 2, pp. 81 582–81 593, 2020.

[5] R. H. Hong, C. Shu, and Q. Y. Zhang, "Security situation prediction method for industrial control network based on adaptive grey verhulst model and gru network," *International Journal of Network Security*, vol. 24, no. 1, pp. 49–61, 2022.

[6] J. R. Jiang and Y. T. Chen, "Industrial control system anomaly detection and classification based on network traffic," *IEEE Access*, vol. 1, no. 2, pp. 41 874–41 888, 2022.

[7] Y. Kang, J. Zhong, and R. Li, "Classification method for network security data based on multi-featured extraction," *International Journal on Artificial Intelligence Tools*, vol. 30, no. 1, p. 2140006, 2021.

[8] S. M. Kasongo and Y. Sun, "Performance analysis of intrusion detection systems using a feature selection method on the unsw-nb15 dataset," *Journal of Big Data*, vol. 7, no. 1, pp. 1–20, 2020.

[9] G. Y. Kim, S. M. Lim, and I. C. Euom, "A study on performance metrics for anomaly detection based on industrial control system operation data," *Electronics*, vol. 11, no. 8, p. 1213, 2022.

[10] Y. Liao, G. Zhao, and J. Wang, "Network security situation assessment model based on extended hidden markov," *Mathematical Problems in Engineering*, vol. 2020, 2020.

[11] E. U. Opara and O. J. Dieli, "Enterprise cyber security challenges to medium and large firms: An analysis," *International Journal of Electronics and Information Engineering*, vol. 13, no. 2, pp. 77–85, 2021.

[12] X. Tang, Q. Zheng, and J. Cheng, "A ddos attack situation assessment method via optimized cloud model based on influence function," *Computers, Materials and Continua*, vol. 60, no. 3, pp. 1263–1281, 2019.

[13] X. Tao, K. Kong, and F. Zhao, "An efficient method for network security situation assessment," *International Journal of Distributed Sensor Networks*, vol. 16, no. 11, p. 1550147720971517, 2020.

[14] X. Tao, Z. Liu, and C. Yang, "An efficient network security situation assessment method based on ae and pmu," *Wireless Communications and Mobile Computing*, vol. 2021, 2021.

[15] W. Wang, F. Shi, and M. Zhang, "A vulnerability risk assessment method based on heterogeneous information network," *IEEE Access*, vol. 8, pp. 148 315–148 330, 2020.

[16] W. Wu and C. Y. Yang, "An overview on network security situation awareness in internet," *International Journal of Network Security*, vol. 24, no. 3, pp. 450–456, 2022.

[17] J. Xue and B. Shen, "A novel swarm intelligence optimization approach: sparrow search algorithm," *Systems Science & Control Engineering*, vol. 8, no. 1, pp. 22–34, 2020.

[18] Y. Xue, "Research on network security intrusion detection with an extreme learning machine algorithm," *International Journal of Network Security*, vol. 24, no. 1, pp. 29–35, 2022.

[19] Y. Xue, "Research on network security intrusion detection with an extreme learning machine algorithm," *International Journal of Network Security*, vol. 24, no. 1, pp. 29–35, 2022.

[20] H. Y. Yang and Z. X. Zhang, "Network security situation assessments with parallel feature extraction and an improved bigru," *Journal of Tsinghua University Science and Technology*, vol. 62, no. 5, pp. 842–848, 2022.

[21] H. Yang, Z. Zhang, and L. Xie, "Network security situation assessment with network attack behavior classification," *International Journal of Intelligent Systems*, vol. 37, no. 10, pp. 6909– 6927, 2022.

[22] Y. Yang, Z. Yang, and Q. Yang, "Network security risk assessment based on enterprise environment characteristics," *International Journal of Network Security*, vol. 24, no. 1, pp. 156–165, 2022.

[23] H. Zhang, C. Kang, and Y. Xiao, "Research on network security situation awareness based on the lstm-dt model," *Sensors*, vol. 21, no. 14, p. 4788, 2021.

[24] Z. W. Zhao, "An evaluation method of network security situation using data fusion theory," *International Journal of Performability Engineering*, vol. 16, no. 7, pp. 1046–1057, 2020.

Biography

Peng-Shou Xie was born in Jan. 1972. He is a professor and a supervisor of a master student at the Lanzhou University of Technology.His major research field is Security on the Internet of Things. E-mail: xiepshlut@163.com

Hong Wang was born in Mar.1995. He is a master student at Lanzhou University of Technology. Her major research field is network and information security. E-mail: 2967589625@qq.com .

Jia-lu Wang was born in Feb. 1998. He is a master student at Lanzhou University of Technology. His major research field is network and information security.

E-mail: 1126334429 @qq.com .

Xiao-Ye Li was born in Feb. 1997. She is a master student at Lanzhou University of Technology. His major research field is network and information security. E-mail: 976339400 @qq.com

Yin-Chang Pan was born in Feb. 1997. He is a master student at Lanzhou University of Technology. His major research field is network and information security. E-mail: 1713974116 @qq.com

Tao Feng was born in Dec. 1970. He is a professor and a supervisor of Doctoral students at Lanzhou University of Technology. His major research field is modern cryptography theory, network, and information security technology. E-mail: fengt@lut.cn

LWE-based Key Encapsulation Mechanism in the Multi-User Setting

Shanshan Zhang[1,2], Yupu Hu[1], and Momeng Liu[3]
(Corresponding author: Shanshan Zhang)

State Key Laboratory of Integrated Services Networks & Xidian University[1]
No. 2, Taibai South Road, Xi'an, Shaanxi Province, P. R. China
School of Mathematics and Information Science & Baoji University of Arts and Science[2]
No. 44, Baoguang Road, Baoji City, Shaanxi Province, P. R. China
School of Computer Science & Xi'an Polytechnic University[3]
No. 19, Jinhua South Road, Xi'an City, Shaanxi Province, P. R. China
Email: sszhang0801@163.com
(Received May 30, 2022; Revised and Accepted May 28, 2023; First Online June 24, 2023)

Abstract

Key encapsulation mechanism (KEM) is an important cryptographic primitive and served as a basic tool in public-key encryption schemes and authenticated key exchange. Most KEMs are built upon the hardness of integer factorization or computing discrete logarithm problem. Given the quantum computing technology, these schemes will be broken down directly in the presence of quantum computer. On the other hand, considering the actual scenario, the security of KEMs should be deployed in a multi-user setting. Therefore, it is essential to construct KEM in the multi-user setting based on post-quantum cryptography. As a subarea of post-quantum cryptography, lattice-based cryptography has some attractive features. Specifically, the learning with errors (LWE) problem has been used as an amazingly versatile basic tool to design cryptographic schemes. In this paper, we primarily focus on constructing a KEM in the multi-user setting and rely on a standard lattice problem in the random oracle model (ROM). We first construct an indistinguishability under chosen plaintext attacks(IND-CPA) secure public-key encryption scheme by using a key exchange scheme proposed by Ding *et al.*, and then applying a variant of Fujisali-Okamoto (FO) transformation with using prefix hashing to obtain an indistinguishability under chosen ciphertext attacks (IND-CCA) secure KEM in the multi-user setting based on the LWE assumption. Finally, the post-quantum security of the presented KEM scheme is discussed in the ROM.

Keywords: Lattice-Based Cryptography; Key Encapsulation Mechanism; Fujisaki-Okamoto Transformation; Learning with Errors

1 Introduction

Key Encapsulation Mechanism (KEM) is an important public-key primitive, which can be found wide applications in theoretic community and real world, such as public-key encryption (PKE) scheme [4, 11, 16] and authenticated key exchange (AKE) protocol [13,17] are built from KEM. A KEM enables two parties to share a secret key. In recent years, with the rapid development of quantum computes, the traditional hard number theory problem such as discrete logarithm problem [15, 25] and the integer factorization problem [12] are vulnerable to quantum computers attacks, it is urgent to find some constructions based on problems that believed to be resistant to quantum attacks. Since lattice-based public hard problem has good asymptotical efficiency and strong security guarantee, we consider construct a KEM based on lattice hardness problem. Furthermore, the traditional security of KEM is considered in a single-user setting. In the network era, KEM schemes should be deployed in multi-user systems. Therefore, it is essential to construct KEM in the multi-user setting based on post-quantum cryptography.

1.1 Our Motivation and Results

In 2012, Ding *et al.* [5] proposed the first provably secure key exchange scheme (called Ding12 KE) based on the learning with errors (LWE) problem, which is introduced by Regev [22]. The decisional LWE problem is to distinguish polynomially many LWE samples of the form $(\mathbf{a}, b \approx< \mathbf{a}, \mathbf{s} >)$ from uniformly random ones, where $\mathbf{a} \leftarrow \mathbb{Z}_q^n$ and $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ are uniformly random. The hardness of LWE can be reduced to the hardness of various worst-case lattice problems. Many cryptography primitives based on LWE have been proposed, such as public

key encryption [18, 22], attribute-based encryption [3, 24] and fully homomorphic encryption [7, 8], etc.

The LWE problem can be interpreted as unstructured lattice problem. There are also algebraically structured lattice problem, such as Ring-LWE [21, 23] and Modul-LWE [14], which are more compact and computationally efficient, but have the potential weakness due to the extra structure. Using plain LWE to construct KEM scheme that is simple and easy to implement. Therefore, our scheme based on the plain LWE problem with conservative parameterizations.

In Ding12 KE, they point out that their protocol can also be easily extended to a more efficient KEM scheme. The motivation of this paper is to build a new KEM using Ding12 KE as a framework and based on LWE problem. In the meaning time, we consider a stronger notion, multi-user setting security that considers the attacker's advantage in breaking the actual scenario.

For these reasons, designing a practical post-quantum secure KEM in the multi-user setting is already desirable and well motivated.

1.2 Related Works

Many indistinguishability under chosen ciphertext attacks (IND-CCA) secure KEM schemes are constructed, but we focus on post-quantum constructions. The National Institute of Standards and Technology (NIST) has initiated to standardize quantum-resistant public-key cryptographic algorithms [20], including key-establishment algorithms. There are seven algorithms for KEM constructions, and CRYSTALS-Kyber, NTRU and SABER are finalists candidates, and FrodoKEM, HQC, and SIKE are alternate candidates. They are constructed by using Fujisali-Okamoto (FO) transformations from an indistinguishability under chosen plaintext attacks (IND-CPA) or one-way against chosen plaintext attacks (OW-CPA) secure PKE schemes, and most of them are based on lattice hardness assumption. FrodoKEM [1] is the only one based on the hardness of plain LWE problem, but it is stated in the single-user setting. In 2021, Duman *et al.* [6] proposed a variant of Fujisali-Okamoto (FO) transformation in the multi-user setting, which is used to CRYSTALS-Kyber and SABER with the propose of protecting against multi-user attacks. In addition, Han *et al.* [9] studied the tight security of some KEM schemes based on discrete logarithm problem in the multi-user setting. Furthermore, NIST calls for the post-quantum standardization schemes with resisting to multi-key attacks as a submission requirement [19].

1.3 Our Contributions

Our main contribution is constructed a KEM in the multi-user setting based on algebraically unstructured lattices. we rely on a standard lattice problem in the random oracle model (ROM). We first construct an IND-CPA secure public-key encryption (PKE) by using Ding12 KE, and then applying a variant of FO transformation to obtain a KEM in the multi-user setting based on the LWE Problem. Finally, the security of the proposed KEM scheme is discussed in the ROM.

For our KEM construction, to obtain the security of KEM in the multi-user setting, the participants′ public key as an input to the hash function.

In terms of computation efficiency, since our KEM scheme is based on a relatively stronger plain LWE assumption, compared to the most existing CCA secure lattice-based KEM construction, our construction need relatively larger matrix dimensions. However, its security can be proved in the actual multi-user scenario and easy to implement.

1.4 Organization

The rest of this paper is organized as follows. In Section 2, we introduce three useful definitions of LWE, PKE and KEM. Then two building blocks are given in Section 3. In Section 4, we construct the KEM scheme in the multi-user setting based on the LWE problem, and the security proof of our KEM scheme is given. Finally, conclusions are given in Section 5.

2 Preliminaries

In this section, we introduce some notations and fundamental definitions.

2.1 Notation

Let $\lambda \in \mathbb{N}$ denote the security parameter throughout this paper. Let bold capital letters be matrices, and bold lowercase letters be vectors in column form. The notation $\mathbf{A}^{\mathrm{T}}$ denotes the transpose of the matrix $\mathbf{A}$. For an integer $q \geq 1$, $\mathbb{Z}_q$ denotes the quotient ring $\mathbb{Z}/q\mathbb{Z}$. Let " $\leftarrow$ " denote sampling an element from some distribution uniformly at random. The discrete Gaussian distribution over $\mathbb{Z}^n$ with width s is denoted by $D_{\mathbb{Z}^n,s}$. The minimum entropy of a discrete random variable X is defined as $H_\infty(X) = -\log(\max_x \Pr[X = x])$.

2.2 Learning with Errors Problem

The LWE problem was introducced by Regev [22], that is a generalization of the learning parity with noise (LPN) problem with larger modulus. The hardness of it can be reduced by a quantum algorithm to some standard problems on lattices in the worst case.

For an integer $q = q(n) \geq 2$ and some probability distribution χ over $\mathbb{Z}_q$, we define $A_{s,\chi}$ as the distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ of the tuples $(\mathbf{a}, c) = (\mathbf{a}, \mathbf{a}^T\mathbf{s} + e)$ where $\mathbf{s}, \mathbf{a} \leftarrow \mathbb{Z}_q^n$ is uniform and $e \leftarrow \chi$, and all operations are performed in $\mathbb{Z}_q$. There are two versions of the LWE problem, search-LWE and decision-LWE, respectively.

Definition 1 (Search-LWE and decision-LWE). *For an integer $q = q(n)$ and a distribution χ on $\mathbb{Z}_q$, for any $\mathbf{s} \in \mathbb{Z}_q^n$, search-LWE finds $\mathbf{s}$ given any independent samples $(\mathbf{a}, c)$ from $A_{s,\chi}$. The goal of decision-LWE is to distinguish between an oracle that returns independent samples from $A_{s,\chi}$ for some uniform $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, and an oracle that returns independent samples from the uniform distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$.*

Regev showed that these two versions are polynomially equivalent for $q = poly(n)$. For certain choices of q and χ, the decision-LWE problem is as hard as solving the shortest independent vectors problem (SIVP) using a quantum algorithm.

Theorem 1. *Let $q = q(n)$ be a prime and let $\alpha = \alpha(n) \in (0, 1)$ such that $\alpha q > 2\sqrt{n}$. If there exists an efficient algorithm that solves the decision-LWE problem, then there exists an efficient quantum algorithm for the SIVP within $\widetilde{O}(n/\alpha)$ in the worst case.*

Due to the hardness of SIVP, we choose the decision-LWE problem as underlying hardness in this paper. It is convenient to write the LWE problem in matrix form, such as collecting the vectors $\mathbf{a}_i \in \mathbb{Z}_q^n$ as the columns of a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, then the LWE instances can be given by $(\mathbf{A}, \mathbf{A}^T\mathbf{s} + \mathbf{e})$, where $\mathbf{s} \in \mathbb{Z}_q^n$, $\mathbf{e} \in \mathbb{Z}_q^m$.

2.3 Public-Key Encryption

A public-key encryption scheme PKE=(Gen, Enc, Dec) consists of three algorithms along with a finite message space $\mathcal{M}$:

Gen(λ): Taking public parameters λ as input, the probabilistic key generation algorithm outputs a public key pk and a secret key sk.

Enc((pk, m)): Taking pk and a message $m \in \mathcal{M}$ as input, the probabilistic encryption algorithm outputs a ciphertext $c \leftarrow \text{Enc}(m, pk; r)$, where r is a random number.

Dec (sk, c)**:** Taking as input sk and c, the deterministic decryption algorithm outputs m' or $\perp$.

A PKE scheme with message space $\mathcal{M}$ is δ correctness if

$$\mathbb{E}[\max_{m \in \mathcal{M}} Pr[Dec(sk, Enc(pk, m)) \neq m]] \leq \delta,$$

where the expectation is taken over $(pk, sk) \leftarrow \text{Gen}(\lambda)$.

If the PKE scheme has n-user, the correctness error is $\delta(n)$ if

$$\mathbb{E}[\max_{i \in [n]} \max_{m \in \mathcal{M}} Pr[Dec(sk_i, Enc(pk_i, m)) \neq m]] \leq \delta(n),$$

where the expectation is taken over $((pk_1, sk_1), \cdots, (pk_n, sk_n)) \leftarrow \text{Gen}^n(\lambda)$.

Generally speaking, the trivial bounds are $\delta \leq \delta(n) \leq n\delta$. For most natural lattice-based scheme such as an LWE-based encryption scheme, we have $\delta(n) < n\delta$ [6].

$\underline{(n, q_C) - \text{IND-CCA}}$
01. for $i \in [n]$
02. $(pk_i, sk_i) \leftarrow \text{Gen}(\lambda)$
03. $\overrightarrow{pk} \leftarrow (pk_1, \ldots, pk_n)$
04. $b \leftarrow \{0, 1\}$
05. $b' \leftarrow \mathcal{A}^{\text{Chall}}(\overrightarrow{pk})$
06. If $b' = b$ then
07. returen 1
08. else
09. return 0

$\underline{\text{Chall}(i, m_0, m_1)}$ /max.q_C queries
10. return $\text{Enc}(pk_i, m_b)$

Figure 1: The game (n, q_C) -IND-CPA for PKE in the n-user/q_C-challenges setting

In terms of security, considering the n-user/q_C-challenges IND-CPA advantages function of an adversary $\mathcal{A}$:

$\text{Adv}_{\text{PKE}}^{(n,q_C)-\text{IND-CPA}}(\mathcal{A})$:

$$= \mid Pr[(n, q_C) - \text{IND-CPA}_{\text{PKE}}^{\mathcal{A}} \Rightarrow 1] - \frac{1}{2} \mid,$$

where the game $(n, q_C) - \text{IND-CPA}$ is defined in Figure 1, and q_C is the number of challenge queries.

2.4 Key Encapsulation Mechanism

A key encapsulation mechanism KEM=(Gen, Encaps, Decaps) is a tuple of algorithms with public secret key spaces $\mathcal{PK} \times \mathcal{SK}$, a finite key space $\mathcal{K}$, and a ciphertext space $\mathcal{C}$.

Gen(λ): Input public parameters λ, the key generation algorithm outputs a pair of public key and secret key (pk, sk).

Encaps(pk): Input public key pk, the encapsulation algorithm outputs a pair of ciphertext $c \in \mathcal{C}$ and encapsulated key $K \in \mathcal{K}$.

Decaps (sk, c)**:** Input secret key sk and ciphertext c, the deterministic decapsulation algorithm outputs $K \in \mathcal{K} \bigcup \{\perp\}$.

Correctness of KEM scheme requires that for all λ, $(pk, sk) \in \text{Gen}\ (pp)$, $(c, K) \in \text{Encaps}(pk)$, such that Decaps (sk, c)=K.

In terms of KEM's security, we consider the n-user/q_C-challenges IND-CCA advantages function of an adversary $\mathcal{A}$:

$\text{Adv}_{\text{KEM}}^{(n,q_C)-\text{IND-CCA}}(\mathcal{A})$:

$$= \mid Pr[(n, q_C) - \text{IND-CCA}_{\text{KEM}}^{\mathcal{A}} \Rightarrow 1] - \frac{1}{2} \mid,$$

where the game $(n, q_C) - \text{IND-CCA}$ is defined in Figure 2, and let C_i describe the set of challenge ciphertexts for participant i.

(n, q_C) – IND-CCA
01. for $i \in [n]$
02. $(pk_i, sk_i) \leftarrow$ Gen
03. $\overrightarrow{pk} \leftarrow (pk_1, \ldots, pk_n)$
04. $b \leftarrow \{0,1\}$
05. $b' \leftarrow \mathcal{A}^{\text{Decap.Chall}}(\overrightarrow{pk})$
06. If $b' = b$, returen 1 ; else, return 0.

Chall(i) /max.q_C queries
07. $(c, K_0) \leftarrow$ Encaps(pk_i)
08. $K_1 \leftarrow \mathcal{K}$
09. $C_i := C_i \bigcup \{c\}$
10. return (c, K_b)

Descaps($i, c \notin C_i$)
11. return Decaps (sk_i, c)

Figure 2: The game (n, q_C) -IND-CCA for KEM in the n-user/q_C-challenges setting

3 Building Blocks

3.1 Ding12 Key Exchange Protocol

Ding12 KE protocol likes the Diffie-Hellman key exchange protocol is based on LWE problem, the specific process is described in Figure 3.

The system first generates the public parameters q, n, α, where $q > 8$ is prime. Sample a uniformly random matrix $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times n}$. Let E be the robust extractor which enables two parties to extract an identical information from two close elements with some additional hint. For any $x, y \in \mathbb{Z}_q$ such that $x - y$ is even and $|x - y| \leq \delta$, then $E(x, \sigma) = E(y, \sigma)$, where the error tolerance $\delta = \frac{q}{4} - 2$ and the signal $\sigma \leftarrow S(y) = \sigma_b(y)$, where $b \leftarrow \{0,1\}$. The robust extractor is defined as follows:

$$E(x, \delta) = (x + \sigma \cdot \frac{q-1}{2} \bmod q) \bmod 2.$$

$\sigma_b(x)$ from $\mathbb{Z}_q$ to $\{0,1\}$ as follows:

$$\sigma_0(x) = \begin{cases} 0, & x \in [-\lfloor \frac{q}{4} \rfloor, \lfloor \frac{q}{4} \rfloor]; \\ 1, & \text{otherwise.} \end{cases} ;$$

$$\sigma_0(x) = \begin{cases} 0, & x \in [-\lfloor \frac{q}{4} \rfloor + 1, \lfloor \frac{q}{4} \rfloor + 1]; \\ 1, & \text{otherwise.} \end{cases} .$$

If two participants run the protocol honestly according to Figure 3, they will share an identical key. Ding12 KE based on LWE assumption is secure against passive probabilistic polynomial-time (PPT) adversaries.

3.2 A Variant of FO Transformation

Let PKE={Gen, Enc, Dec} be a public-key encryption scheme with message space $\mathcal{M}$, public-key space $\mathcal{PK}$, randomness space $\mathcal{R}$, and ciphertext space $\mathcal{C}$. The FO transformation [10] can only offer security in a single user setting. In the FO transformation, a hash function H does not include any part of public key, which is modeled as a random oracle, that mainly used to derive the PKE randomness r and the encapsulation key K. Let $\text{FO}^{\not\perp}$ be FO with implicit rejection. A variant of $\text{FO}^{\not\perp}$ transformation $\text{FO}^{\not\perp}_{\text{ID}(pk),m}$ with prefix hashing is proposed in [6], which can transform a passively secure PKE scheme into an actively secure KEM. Let ID: $\mathcal{PK} \rightarrow \{0,1\}^t$ be a fixed-output length function and H:$\{0,1\}^* \rightarrow \{0,1\}^k \times \mathcal{R}$ be a Hash function, where H_1(X) is defined as the first k bits of H(X). The KEM with $\text{FO}^{\not\perp}_{\text{ID}(pk),m}$ is described in Figure 4, where $\text{FO}^{\not\perp}_{\text{ID}(pk),m}$ is essentially $\text{FO}^{\not\perp}_{m}$ with ID(pk) into the hash function H and l is the length of the secret seed s.

4 IND-CCA Secure KEM in the Multi-user Setting

In this section, we first propose a public-key encryption scheme labled with DingPKE, targeting IND-CPA security, that based on the Ding12 KE and will be used as a building block for achieving IND-CCA security KEM. DingPKE does not use any reconciliation mechanism that was proposed in [5]. IND-CPA security of DingPKE is based on the public-key encryption scheme presented by Lindner and Peikert [18], which uses "Encode" and "Decode" pattern. DingPKE scheme is given by three algorithms (DingPKE.Gen, DingPKE.Enc, DingPKE.Dec), defined as follows and further shown in Figure 5, where Encode(μ)=$\mu \cdot \lfloor \frac{q}{2} \rfloor$, and Decode($c$)=0, if $c \in [-\lfloor \frac{q}{4} \rfloor, \lfloor \frac{q}{4} \rfloor) \subset \mathbb{Z}_q$ and 1 otherwise. Suppose two participants Alice and Bob decide to secure communication by using DingPKE over an open channel.

DingPKE.KeyGen(q, n, α): The public parameters are q, n, α, where $q > 2$ is a prime. Sample a uniformly random matrix $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times n}$, $\mathbf{s}_i, \mathbf{e}_i \leftarrow \mathcal{D}_{\mathbb{Z}^n, \alpha q}$. Then, Alice compute $\mathbf{p}_i = \mathbf{A} \cdot \mathbf{s}_i + \mathbf{e}_i \bmod q$. The public key is $\mathbf{p}_i$, the secret key is $\mathbf{s}_i$.

DingPKE.Enc($\mathbf{p}, \mu$): Bob chooses two vectors $\mathbf{s}_j, \mathbf{e}_j \leftarrow \mathcal{D}_{\mathbb{Z}^n, \alpha q}$ and an error vector $\mathbf{e'}_j \leftarrow \mathcal{D}_{\mathbb{Z}, \alpha q}$, compute $\mathbf{c_1} = \mathbf{A}^T \cdot \mathbf{s}_j + e_j \bmod q$ and $\mathbf{c_2} = \mathbf{p}_i^T \cdot \mathbf{s}_j + \mathbf{e'_j} + \text{Encode}(\mu) \bmod q$.

DingPKE.Dec($\mathbf{c}, \mathbf{s}$): Once receiving $(\mathbf{c_1}, \mathbf{c_2})$, Alice computes $m = \mathbf{c_2} - \mathbf{s}_i^T \mathbf{c_1}$ and returns $\mu' \leftarrow \text{Decode}(m)$.

Correctness of decryption: The decryption algorithm DingPKE.Dec computes DingPKE uses "Encode" and "Decode" pattern, it is required an error-tolerant t, that is, for any integer $e \in [-t, t)$, the equation Decode(Encode(μ)+ $e \bmod q$) = μ is satisfied. The lemma 1 states bounds on the size of errors that can be handled by the decoding algorithm.

Lemma 1. *Let $q > 2$ be a prime. Then Decode(Encode(μ)+e mod q) = μ for any $\mu, e \in \mathbb{Z}$ such that $\mu \in \{0,1\}$ and $e < \frac{q}{4}$.*

Alice		Bob
$\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times n}$ $\mathbf{s}_i, \mathbf{e}_i \leftarrow \mathcal{D}_{\mathbb{Z}^n,\alpha q}$ $\mathbf{p}_i = \mathbf{A}\cdot\mathbf{s}_i + 2\mathbf{e}_i \bmod q$	$\xrightarrow{\mathbf{p}_i}$	$\mathbf{s}_j, \mathbf{e}_j \leftarrow \mathcal{D}_{\mathbb{Z}^n,\alpha q}$ $\mathbf{p}_j = \mathbf{A}^T\cdot\mathbf{s}_j + 2\mathbf{e}_j \bmod q$ $\mathbf{e'}_j \leftarrow \mathcal{D}_{\mathbb{Z},\alpha q}$ $\mathbf{k}_j = \mathbf{p}_i^T\cdot\mathbf{s}_j + 2\mathbf{e'}_j \bmod q$ $\sigma \leftarrow \mathbf{S}(\mathbf{k}_j)$ $\mathbf{S}(\mathbf{k}_j) = E(\mathbf{k}_j, \sigma)$
	$\xleftarrow{\mathbf{P}_j, \sigma}$	
$\mathbf{e'}_i \leftarrow \mathcal{D}_{\mathbb{Z},\alpha q}$ $\mathbf{k}_i = \mathbf{s}_i^T\cdot\mathbf{P}_j + 2\mathbf{e'}_i \bmod q$ $\mathbf{S}(\mathbf{k}_i) = E(\mathbf{k}_i, \sigma)$		

Figure 3: Ding12 KE based on LWE problem

$\underline{\text{Gen}'}$
01. $(pk, sk) \leftarrow \text{Gen}$
02. $s \leftarrow \{0,1\}^l$
03. $sk' := (sk, s)$
04. return (pk, sk')

$\underline{\text{Encasps}(pk)}$
05. $m \leftarrow \mathcal{M}$
06. $(K, r) \leftarrow H(\text{ID}(pk), m)$
07. $c \leftarrow \text{Enc}(pk, m; r)$
08. return (K, c)

$\underline{\text{Decaps}((sk, s), c)}$
09. $m' \leftarrow \text{Dec}(sk, c)$
10. $(K, r) \leftarrow \text{H}(\text{ID}(pk), m')$
11. $K' \leftarrow \text{H}_1(\text{ID}(pk), s, c)$
12. If $m' = \perp$ or $\text{Enc}(pk, m'; r) \neq c$ return K'
13. else return K

Figure 4: KEM = $\text{FO}^{\not\perp}_{\text{ID}(pk),m}$ [PKE, ID, H]

This lemma follows directly from the fact that Decode(Encode(μ)+e)=$\lfloor \mu + \frac{2}{q} \rfloor \bmod 2$.

For the correctness, we analysis the reasonable way to select the parameters of DingPKE. The decryption algorithm of DingPKE computes

$$\begin{aligned} m &= \mathbf{c_2} - \mathbf{s}_i^T\mathbf{c_1} \\ &= \mathbf{k}_j + \mathsf{Encode}(\mu) - \mathbf{s}_i^T\mathbf{p}_j \\ &= \mathbf{p}_i^T\mathbf{s}_j + \mathbf{e}_j^{'} + \mathsf{Encode}(\mu) - \mathbf{s}_i^T(\mathbf{A}^T\mathbf{s}_j + \mathbf{e}_j) \\ &= (\mathbf{A}\mathbf{s}_i + \mathbf{e})_i)^T\mathbf{s}_j + \mathbf{e}_j^{'} + \mathsf{Encode}(\mu) - \mathbf{s}_i^T\mathbf{A}^T\mathbf{s}_j - \mathbf{s}_i^T\mathbf{e}^j \\ &= \mathbf{s}_i^T\mathbf{A}^T\mathbf{s}_j + \mathbf{e}_i^T\mathbf{s}_j + \mathbf{e}_j^{'} + \mathsf{Encode}(\mu) - \mathbf{s}_i^T\mathbf{A}^T\mathbf{s}_j - \mathbf{s}_i^T\mathbf{e}^j \\ &= (\mathbf{e}_i^T\mathbf{s}_j + \mathbf{e}_j^{'} - \mathbf{s}_i^T\mathbf{e}_j) + \mathsf{Encode}(\mu) \end{aligned}$$

Let $e = \mathbf{e}_i^T\mathbf{s}_j + \mathbf{e}_j^{'} - \mathbf{s}_i^T\mathbf{e}_j$, the message μ corresponding to an entry of m will be decrypted correctly if the condition in Lemma 1 is satisfied for the corresponding entry of e.

Theorem 2. *The DingPKE is IND-CPA secure, assuming the hardness of the LWE problem.*

Proof. We prove the security by showing the entire view of a PPT adversary in an IND-CPA is computationally indistinguishable from uniformly random. For any encrypted message $\mu \in \{0,1\}$, the view consists of $(\mathbf{A}, \mathbf{p}_i, \mathbf{c})$, where $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times n}$ is uniformly random, $\mathbf{p}_i = \mathbf{A}\cdot\mathbf{s}_i + \mathbf{e}_i \bmod q$, and $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2)$. Let $\mathbf{p}_i^*$ be uniform, then $(\mathbf{A}, \mathbf{p}_i)$ is computationally indistinguishable from $(\mathbf{A}, \mathbf{p}_i^*)$ under the assumption of the LWE. Let $\mathbf{c}^*$ be uniform, then $(\mathbf{A}, \mathbf{p}_i, \mathbf{c})$ is also computationally indistinguishable from $(\mathbf{A}, \mathbf{p}_i^*, \mathbf{c}^*)$ under the LWE problem, because $\mathbf{c}_1 = \mathbf{A}^T\cdot\mathbf{s}_j + e_j \bmod q$ and $\mathbf{c}_2 = \mathbf{p}_i^T\cdot\mathbf{s}_j + \mathbf{e'_j} + \text{Encode}(\mu) \bmod q$, where $\mathbf{s}_j, \mathbf{e}_j \leftarrow \mathcal{D}_{\mathbb{Z}^n,\alpha q}$ and $\mathbf{e'}_j \leftarrow \mathcal{D}_{\mathbb{Z},\alpha q}$. Therefore, Any PPT adversary can not distinguish $(\mathbf{A}, \mathbf{p}_i, \mathbf{c})$ and $(\mathbf{A}, \mathbf{p}_i^*, \mathbf{c}^*)$, if the LWE assumption holds. □

Alice		Bob
$\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times n}$		
$\mathbf{s}_i, \mathbf{e}_i \leftarrow \mathcal{D}_{\mathbb{Z}^n,\alpha q}$		$\mathbf{s}_j, \mathbf{e}_j \leftarrow \mathcal{D}_{\mathbb{Z}^n,\alpha q}$
$\mathbf{p}_i = \mathbf{A}\cdot\mathbf{s}_i + \mathbf{e}_i \bmod q$	$\xrightarrow{\mathbf{p}_i}$	$\mathbf{c}_1 = \mathbf{A}^T\cdot\mathbf{s}_j + \mathbf{e}_j \bmod q$
		$\mathbf{e'}_j \leftarrow \mathcal{D}_{\mathbb{Z},\alpha q}$
		$\mathbf{c}_2 = \mathbf{p}_i^T\cdot\mathbf{s}_j + \mathbf{e'}_j + \mathrm{Encode}(\mu) \bmod q$
	$\xleftarrow{\mathbf{c}}$	$\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2)$
$m = \mathbf{c}_2 - \mathbf{s}_i^T\mathbf{c}_1$		
$\mu' \leftarrow \mathrm{Decode}(m)$		

Figure 5: DingPKE sheme

Lemma 2. *Let $Adv_{PKE}^{IND\text{-}CPA}$ be the security advantages of DingPKE, and $Adv_{PKE}^{(n,q_C)-IND\text{-}CPA}$ is the security advantages of n-user DingPKE, according to the argument in [2], one can obtain the trivial bounds*

$$Adv_{PKE}^{IND\text{-}CPA} \le Adv_{PKE}^{(n,q_C)-IND\text{-}CPA} \le n\cdot q_C Adv_{PKE}^{IND\text{-}CPA}$$

where q_C is the number of challenges.

The n-user DingPKE scheme with security against CPA is constructed, and then applying the $\mathrm{FO}^{\not\perp}_{\mathrm{ID}(pk),m}$ transformation, we can obtain an LWE-based KEM scheme in the multi-user setting. Our LWE-based KEM in n-user setting as in Figure 6.

Theorem 3. *For any adversary $\mathcal{A}$ against the $(n, q_C)-$ IND-CCA security of KEM:=$FO^{\not\perp}_{ID(pk),m}$[PKE, ID, H], there exist adversaries $\mathcal{B}$ against $(n, q_C)-$ IND-CPA of DingPKE, such that*
$Adv_{KEM}^{(n,q_C)-IND\text{-}CCA}(\mathcal{A}) \le 2Adv_{DingPKE}^{(n,q_C)-IND\text{-}CPA}(\mathcal{B})$
$+\frac{2(q_H+q_C)q_C}{|\mathcal{M}|} + \frac{q_H}{2^l} + (q_H+q_D)\cdot\delta(n) + \frac{n^2}{2^h}$.
where q_H is the number of ROM queries, q_D is the number of decapsulation queries, q_D is the number of challenge queries, l is the length of the secret seed s, and l is the minimum entropy of ID(PK), i.e., $h = H_\infty(pk)$.

Accoding to Theorem 3 (Theorem 3.1 in [6]), our KEM scheme in the multi-user setting is IND-CCA secure as long as DingPKE is IND-CPA secure.

5 Conclusions

Most KEM schemes were proposed to offer security in a single user setting, and some of them can not resist quantum attack. In this paper, we first construct an IND-CPA secure DingPKE based on Ding12 KE, and give the security proof. Furthermore, LWE-based KEM in multi-user setting are proposed by applying the FO transformation $\mathrm{FO}^{\not\perp}_{\mathrm{ID}(pk),m}$, and the security of the KEMs achieve IND-CCA-secure. The plain LWE problem has a few requirements on it parameters, which is easy to

$\underline{\mathrm{Gen}'}$
01. for $i \in n$
02. $(pk_i, sk_i) \leftarrow$ Gen
03. $s_i \leftarrow \{0,1\}^\lambda$
04. $sk'_i := (sk_i, s_i)$
05. $\overrightarrow{pk} \leftarrow (pk_1, pk_2, \ldots, pk_n)$
06. $\overrightarrow{sk'} \leftarrow (sk'_1, sk'_2, \ldots, sk'_n)$
07. return $(\overrightarrow{pk}, \overrightarrow{sk'})$

$\underline{\mathrm{Encasps}(\overrightarrow{pk})}$
08. $m_i \leftarrow \mathcal{M}$
09. $(K_i, r_i) \leftarrow H(\mathrm{ID}(pk_i), m_i)$
10. $c_i \leftarrow \mathrm{DingPKE.Enc}(pk_i, m_i; r_i)$
11. $\overrightarrow{K} \leftarrow (K_1, K_2, \ldots, K_n)$
12. $\overrightarrow{c} \leftarrow (c_1, c_2, \ldots, c_n)$
13. return $(\overrightarrow{K}, \overrightarrow{c})$

$\underline{\mathrm{Decaps}(\overrightarrow{sk'}, c)}$
14. $m'_i \leftarrow \mathrm{DingPKE.Dec}(sk_i, c_i)$
15. $(K_i, r_i) \leftarrow \mathrm{H}(\mathrm{ID}(pk_i), m'_i)$
16. $K'_i \leftarrow \mathrm{H}_1(\mathrm{ID}(pk_i), s_i, c_i)$
17. If $m' = \perp$
or $\mathrm{DinPKE.Enc}(pk_i, m'_i; r_i) \neq c_i$
return K'_i
18. else return K_i

Figure 6: LWE-based KEM in the n-user setting

meet almost desired security target. The KEM whether achieves IND-CCA security in the quantum random-oracle model (QROM) should be considered. In addition, Ring-LWE and Module-LWE problems on random algebraically structured lattices over certain polynomial rings can make high efficient. Therefore, we will study KEM in the multi-user setting based on Ring-LWE or Module-LWE problems. Moreover, based-lattice KEM with tight enhanced security in the multi-user setting whether exist should be considered as our follow-on work.

Acknowledgments

This work was supported by the National Natural Science Foundations of China (Grant Nos. 61972457, 61902303), the MOE Layout Foundation of Humanities and Social Sciences (Grant No. 19YJA790007), the Natural Science Basic Research Plan in Shaanxi Province of China (Grant Nos. 2019JM-291, 2021JM-514), the Scientific Research Program Funded by Shaanxi Provincial Education Department (Grant No. 21JK0651), the Young Talent fund of University Association for Science and Technology in Shaanxi, China (Grant No. 20210116), and the Shaanxi Key Laboratory of Blockchain and Secure Computing (Grant No. N-KY-XZ-1101-202110-7349). We would like to thank the anonymous reviewers for their valuable comments.

References

[1] E. Alkim, J. W. Bos, Lé. Ducas, K. Easterbrook, B. LaMacchia, P. Longa, I. Mironov, M. Naehrig, V. Nikolaenko, C. Peikert, A. Raghunathan, and D. Stebila, "FrodoKEM: Learning with errors key encapsulation," in *Submission to the NIST Post-Quantum Cryptography standardization project, Round 3*, https://frodokem.org/, 2020.

[2] M. Bellare, A. Boldyreva, and S. Micali, "Public-key encryption in a multi-user setting: Security proofs and improvements," in *Advances in Cryptology – EUROCRYPT 2000*, pp. 259–274, 2000.

[3] X. Boyen, "Attribute-based functional encryption on lattices," in *Theory of Cryptography Conference*, pp. 122–142, Tokyo, Japan, 2013.

[4] R. Cramer and V. Shoup, "Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack," *SIAM J. Comput*, vol. 33, no. 1, pp. 167–226, 2003.

[5] J. Ding, X. Xie, and X. Lin, "A simple provably secure key exchange scheme based on the learning with errors problem," *Cryptology ePrint Archive, Report 2012/688*, 2012.

[6] J. Duman, K. Hovlamnns, E. kilta, V. Lyubashecsky, and G. Seiler, "Fast lattice-based kem svia a gneric fujisaki-okamoto transform using prefix hashing," in *In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Securityl*, pp. 2722–2737, 2021.

[7] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *STOC 2009*, pp. 169–178, Bethesda, Maryland, USA, 2009.

[8] S. Gorbunov S. Halevi V. Nikolaenko G. Segev V. Vaikuntanathan D. Boneh, C. Gentry and D. Vinayagamurthy, "Fully key-homomorphic encryption, arithmetic circuit abe, and compact garbled circuits," in *Advances in Cryptology-EUROCRYPT 2014*, pp. 533–556, Copenhagen, Denmark, 2014.

[9] S. Han, S. Liu, and D. Gu, "Key encapsulation mechanism with tight enhanced security in the multi-user setting: Impossibility result and optimal tightness," in *Advances in Cryptology – ASIACRYPT (2) 2021*, pp. 483–513, 2021.

[10] D. Hofheinz, K. Hövelmanns, and E. Kiltz, "A modular analysis of the fujisaki-okamoto transformation," in *TCC*, pp. 341–371, 2017.

[11] S. T. Hsu, C. C. Yang, and M. S. Hwang, "A study of public key encryption with keyword search", *International Journal of Network Security*, vol. 15, no. 2, pp. 71-79, Mar. 2013.

[12] M. S. Hwang, Chao-Chen Yang, S. F. Tzeng, "Improved digital signature scheme based on factoring and discrete logarithms", Journal of Discrete Mathematical Sciences & Cryptography, vol. 5, no. 2, pp. 151-155, 2002.

[13] T. Jager, E. Kiltz, D. Riepel, and S. Schage, "Tightly-secure authenticated key exchange, revisited," in *Advances in Cryptology – EUROCRYPT 2021*, pp. 117–146, 2021.

[14] A. Langlois and D. Stehl, "Worst-case to average-case reductions for module lattices," *Designs, Codes and Cryptography*, vol. 75, no. 3, pp. 565–599, 2015.

[15] C. C. Lee, M. S. Hwang, L. H. Li, "A new key authentication scheme based on discrete logarithms", *Applied Mathematics and Computation*, vol. 139, no. 2, pp. 343-349, July 2003.

[16] C. T. Li, M. S. Hwang, "A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks",*Information Sciences*, vol. 181, no. 23, pp. 5333-5347, 2011.

[17] I. C. Lin, C. C. Chang, M. S. Hwang, "Security enhancement for the simple authentication key agreement algorithm", in *Proceedings 24th Annual International Computer Software and Applications Conference (COMPSAC'00)*, 2000.

[18] R. Lindner and C. Peikert, "Better key sizes (and attacks) for lwe-based encryption," in *Topics in Cryptology - CT-RSA 2011*, pp. 319–339, Santa Barbara, 2011.

[19] NIST, "Submission requirements and evaluation criteria for the postquantum cryptography standardization process," in *https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposalsfinal-dec-2016.pdf*, 2016.

[20] NIST, "Post-quantum cryptography: Round 3 submissions," in *https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions*, 2020.
[21] C. Peikert V. Lyubashevsky and O. Regev, "On ideal lattices and learning with errors over rings," *Journal of the ACM*, vol. 60, no. 6, pp. 1–35, 2013.
[22] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proc. 37th Annual ACM Symp. on Theory of Computing*, pp. 84–93, 2005.
[23] O. Regev, C. Peikert and N. Stephens-Davidowitz, "Pseudorandomness of ring-lwe for any ring and modulus," in *49th Annual ACM Symposium on Theory of Computing*, pp. 461–473, 2017.
[24] V. Vaikuntanathan S. Gorbunov and H. Wee, "Attribute-based encryption for circuits," in *ACM Symposium on Theory of Computing*, pp. 545–554, Palo Alto, USA, 2013.
[25] C. C. Yang, T. Y. Chang, M. S. Hwang, "A new anonymous conference key distribution system based on the elliptic curve discrete logarithm problem," *Computer Standards & Interfaces*, vol. 25, no. 2, pp. 141-145, 2003.

Biography

Shanshan Zhang received her B.S. degree in 2004 from Baoji University of Arts and Sciences, and received her M.S. degree in 2007 from Huaibei Normal University. Now she is a PhD student in Xidian University. Her main research interests include lattice-based public key -cryptography and indistinguishable obfuscation.

Yupu Hu received the B.S. and M.S. degrees in mathematics from Xidian University, China, in 1987 and 1999, respectively, and the Ph.D. degree in cryptography from Xidian University, in 1999. He is currently a Professor and a Doctoral Supervisor with the School of Telecommunications Engineering, Xidian University. His research interests include analyzing and constructing schemes built upon lattice-based cryptography, multilinear map, and fully homomorphic encryption schemes.

Momeng Liu received the B.S. degree in telecommunications from Xi'an University, China, in 2010, and the M.S. and Ph.D. degrees in cryptography from Xidian University, China, in 2013 and 2018, respectively. She is currently a Lecturer with the School of Computer Science, Xi'an Polytechnic University, China, and a member of the Shaanxi Key Laboratory of Clothing Intelligence, Xi'an Polytechnic University. Her research interest includes analyzing and designing protocols built upon lattice-based cryptography

Vulnerability Identification and Detection of Different Software Codes with a Graph Neural Network

Lei Zhang and Zehui Liu
(Corresponding author: Zehui Liu)
Department of Computer Information Engineering, Baoding Vocational and Technical College
Baoding 071051, China
zaihui260@yeah.net
(Received May 8, 2022; Revised and Accepted May 23, 2023; First Online June 24, 2023)

Abstract

Software vulnerabilities can have a significant impact on the security of software operations. Consequently, for subsequent repair, accurate detection of these vulnerabilities is required. This paper briefly introduced conventional vulnerability detection approaches and the graph neural network-based vulnerability detection algorithm. The software's source code was abstracted into a node graph structure in the graph neural network-based algorithm, thus ensuring the structural integrity of the code. Simulation experiments were then conducted, and the results were compared with the other two algorithms, namely, support vector machine and long short-term memory. It was found that the graph neural network-based algorithm converged to better parameters more quickly during the training stage; the graph neural network-based vulnerability detection algorithm had higher detection accuracy and consumed the least detection time.

Keywords: Code Vulnerability; Graph Neural Network; Graph Structure; Recognition and Detection

1 Introduction

The main manifestation of the Internet in everyday life is various application software [5]. These software are composed of code written in programming languages that are suitable for each software development process. The code that constitutes programming languages is different from natural languages, with a prescribed format that is not as natural as natural languages [2]. However, programming languages are also a type of language, with certain "syntax" rules that programmers need to follow when programming software.

During the editing process, programmers may make writing errors that result in vulnerabilities in the software, and the shortcomings of the "grammar" structure of the programming language may also lead to vulnerabilities [13]. In short, software edited with programming languages may have more or less vulnerabilities, and once these vulnerabilities are exploited by illegal elements, they can cause huge losses to users.

Traditional vulnerability detection methods detect code by manually defined detection rules, but the number of manually defined detection rules is limited [7], and the rules lack a unified standard, making it difficult to construct detection rules that are highly compatible with programs.

With the development of machine learning algorithms, they have been gradually applied to detect static code vulnerabilities [4]. Although machine learning algorithms are now significantly more efficient than traditional static code vulnerability detection techniques and do not require the manual setting of vulnerability detection rules, they still have some drawbacks [14]. Relevant studies are reviewed below.

A new learning framework called FUNDED was proposed by Wang *et al.* [9] for building vulnerability detection models. They found that FUNDED was significantly better than other methods in various evaluation environments.

Ghaffarian [3] proposed a primitive neural vulnerability analysis method that used a custom intermediate graph representation of the program to train the graph neural network model. Software vulnerability analysis tasks were successfully completed using the proposed approach, as demonstrated by the experimental results.

Hu *et al.* [4] proposed a novel and effective vulnerability feature-based method for detecting vulnerabilities in memory. The results of their experiments demonstrated the viability and efficacy of the proposed method.

2 Vulnerability Identification Algorithm Based on Graph Neural Networks

Neural networks, which are a type of deep learning algorithm, have been gradually applied to the detection of code vulnerabilities with the advancement of computer performance and deep learning algorithms [11]. When using deep learning algorithms to detect vulnerabilities, code feature vectors can also be extracted, and then a classification model trained by deep learning algorithms can be used to identify the code. This is similar to the vulnerability detection method based on vulnerability classification models mentioned above. Compared to the classification models trained by machine learning algorithms, deep learning algorithms can uncover deeper hidden patterns, but when extracting feature vectors from code, they still process it in a sequential text-based manner, thus also ignoring the structural information of the code itself [1].

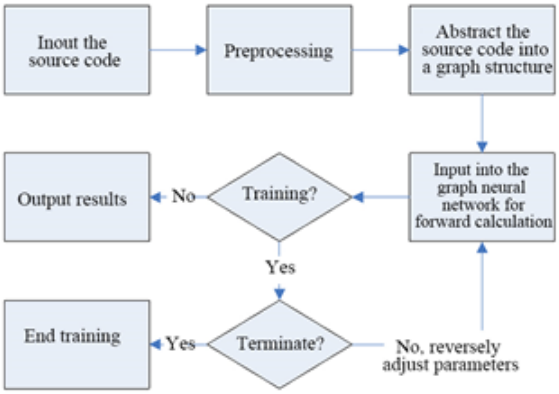


Figure 1: The vulnerability identification process based on graph neural networks

Graph neural networks are also a type of deep learning algorithm. Compared to other types of neural networks, they are more suitable for training and processing graph-structured data [8]. Therefore, when using graph neural networks for vulnerability detection on source code, the source code is first abstracted and transformed into a graph structure composed of nodes and connections. Then, the graph neural network performs forward calculation on the graph structure, obtains the graph structure feature vectors, and performs classification recognition on the fully connected layer. Figure 1 shows the basic flow of the vulnerability identification algorithm based on graph neural networks.

1) The source code that needs to be checked is entered and preprocessed [6]. The purpose of preprocessing is to standardize the code written by different programmers, minimizing the interference caused by programmer writing styles, such as naming conventions and statement usage. The first step of preprocessing is to traverse the code and expand the macro definitions. Afterwards, a mapping table is used to map the custom identifiers in the code to standard symbols. Some of the mapping rules are "user-defined variable names are mapped to VAR_n, where n depends on the order in which the variable names appear", "user-defined function names are mapped to $FUNCTION_n$, where n depends on the order in which the function names appear", and "the variable values in assignment statements are mapped to $VALUE_n$, where n depends on the order in which the variable values appear".

2) The standardized source code is abstracted into a graph structure [10]. Firstly, each line of the source code is viewed as a node, and the node stores the data code (such as variable names and function names) processed by standardization. Then, the control flow of the execution program code is obtained using the abstract syntax tree method, and the connections between the nodes depend on the path of the control flow. After constructing the abstract node graph of the source code, Word2vec is used to vectorize the data code stored in the nodes.

3) The abstract node graph of the source code is input into a graph neural network for forward computation. The corresponding formula is:

$$\begin{cases} h^{l+1} & = f(D^{-\frac{1}{2}}\bar{A}D^{-\frac{1}{2}}h^l\omega^l) \\ \bar{A} & = A + I_N \end{cases} \quad (1)$$

where h^l represents the feature matrix of the l-th hidden layer in the graph neural network, h^{l+1} is the feature matrix of the $l+1$-th hidden layer in the graph neural network, i.e., the output of the previous layer, A is the graph adjacency matrix [12], I_N is the identity matrix of the nodes used for self-looping, N is the number of nodes in the graph structure, $\bar{A}$ represents the graph adjacency matrix after adding self-looping, and ω^l is the trainable parameter matrix of the l-th hidden layer in the graph neural network.

4) After layer-by-layer calculations by the graph neural network, a feature matrix of the abstract graph structure of the source codes is obtained, and then the source codes are classified and output using the softmax function in the fully connected layer. It is determined whether the algorithm is in the training phase at this time. If it is not in the training phase, the classification result is output directly.

5) It is determined whether the algorithm has reached the termination condition if the algorithm is in the training phase. The training is finished if it is reached. If it is not reached, the weight parameters in the hidden layer of the graph neural network are adjusted in reverse based on the classification error, followed by layer-by-layer calculations. The termination conditions include reaching the preset number

of training iterations and the classification error converging within the preset threshold range.

3 Simulation Experiment

3.1 Experimental Data

The data required for the simulation experiment in this paper comes from the SARD database, which contained five types of vulnerabilities, namely CWE-125 for out-of-bound reads, CWE-20 for improper input validation, CWE-190 for integer overflow, CWE-399 for resource management errors, and CWE-400 for resource exhaustion. 2,000 pieces of the data code were collected for each type of vulnerability, and a total of 10,000 pieces of code data with vulnerabilities was collected. At the same time, 10,000 pieces of code data that have been verified to be free of vulnerabilities were collected from an open source project platform as positive samples.

3.2 Experimental Setup

When training the graph neural network algorithm in this paper, batch training was used. The batch size was set to 128, the number of vector dimensions of Word2vec was set to 256, the maximum epoch was set to 100, and the activation function was the Relu function. The learning rate was set to 0.01. Random gradient descent was used to adjust the parameters. Dropout was set to 0.3 to prevent overfitting.

The relevant parameters of support vector machine (SVM) used for comparative experiments are shown below. The penalty parameter was set to 1, and the sigmoid function was used as the kernel function. The following are the relevant parameters of long short-term memory (LSTM). There were 64 hidden neurons, and the maximum epoch during the training process was set to 100. In addition, both detection algorithms detected the code text after Word2vec vectorization, and the number of vector dimension of Word2vec was also set to 256.

3.3 Evaluation Metrics

The widely used indicators were used for evaluating the performance of the code vulnerability detection model, namely accuracy, recall rate, and F-value. Their calculation formulas are:

$$\begin{aligned} P &= \frac{TP}{TP+FP} \\ R &= \frac{TP}{TP+FN} \\ F &= \frac{2PR}{P+R} \end{aligned} \tag{2}$$

where P denotes precision, R denotes recall rate, F denotes the comprehensive consideration, TP denotes the number of positive samples predicted to be positive, FP represents the number of negative samples predicted to be positive, and FN means the number of positive samples predicted to be negative.

3.4 Experimental Results

In the comparative experiment, the SVM algorithm used training data to fit and obtain the "hyperplane" that divided the code categories, while the LSTM and graph neural network algorithms required repeated iterative training to gradually adjust the parameters in the hidden layers to improve detection performance. Figure 2 illustrates the change curve of accuracy and training loss during the training process of the LSTM and graph neural network algorithms. The accuracy and training loss of the LSTM algorithm converged to stability after about 55 iterations, while the graph neural network algorithm converged to stability after about 30 iterations. In addition, whether during the convergence process or after convergence stability, the vulnerability detection algorithm based on the graph neural network had higher accuracy and smaller training loss.

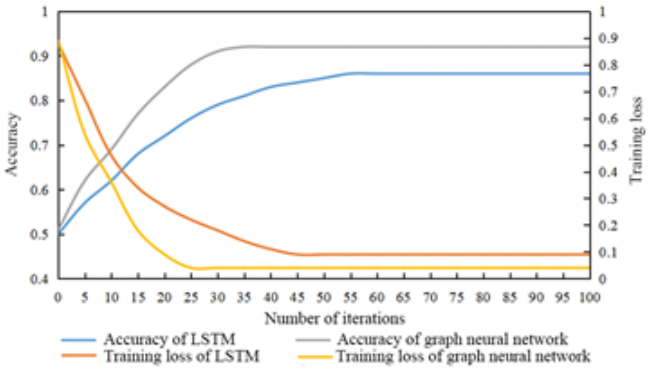


Figure 2: Training curves of the LSTM-based and graph neural network-based vulnerability detection algorithms

To verify the performance of the graph neural network algorithm, it was compared with two detection algorithms, SVM and LSTM. The detection performance of the three vulnerability detection algorithms for different vulnerability types was tested, as shown in Table 1. It was seen from Table 1 that for different types of vulnerabilities, the algorithms had different recommended performance. The SVM algorithm had relatively good detection performance for CWE-190 type vulnerabilities among the five types of vulnerabilities. The LSTM algorithm had relatively good detection performance for CWE-399 type vulnerabilities. The graph neural network has relatively good detection performance for CWE-125 type vulnerabilities. Table 1 also shows the detection time consumption of the three vulnerability detection algorithms for different vulnerability types. It was seen that there was little difference in the detection time consumption between different detection algorithms for different types of vulnerabilities, but it was clearly shown that the graph neural

network-based algorithm had less time consumption.

According to Figure 3, the SVM algorithm had a detection accuracy of 0.68, a recall rate of 0.58, and an F-value of 0.63; the LSTM algorithm had a detection accuracy of 0.87, a recall rate of 0.75, and an F-value of 0.81; the graph neural network algorithm had a detection accuracy of 0.95, a recall rate of 0.86, and an F-value of 0.91. The comparison showed that the graph neural network algorithm had the highest detection accuracy, followed by the LSTM algorithm, and the SVM algorithm had the lowest.

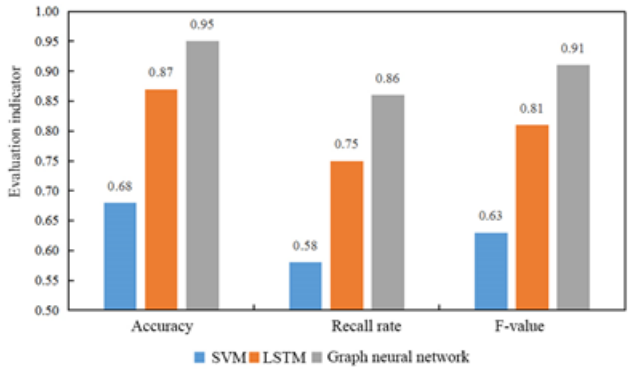


Figure 3: Average detection performance of three vulnerability detection algorithms for vulnerabilities

The average detection time of three vulnerability detection algorithms is shown in Figure 4. The average detection time of the the SVM algorithm was 1.97 s, that of the LSTM algorithm was 1.11 s, and that of the graph neural network algorithm was 0.31 s. From the comparison in Figure 4, it was seen that the SVM algorithm had the longest detection time, followed by the LSTM algorithm, and the graph neural network algorithm had the shortest detection time.

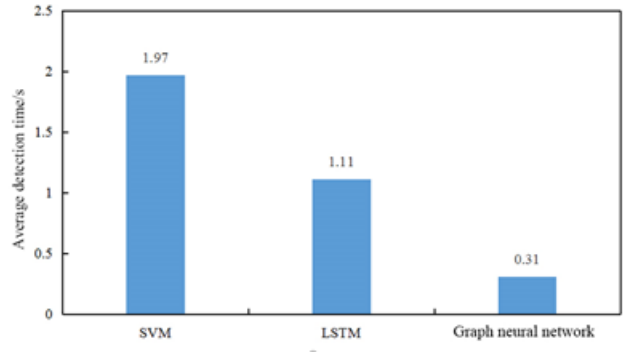


Figure 4: Average detection time of three vulnerability detection algorithms

4 Conclusion

This article briefly introduced traditional vulnerability detection methods and a vulnerability detection algorithm based on a graph neural network. In this algorithm, the source code of the software was abstracted into a node-graph structure, thus ensuring the integrity of the code structure. Then, simulation experiments were carried out, and the proposed algorithm was compared with two other detection algorithms, SVM and LSTM. The results are shown below.

1) After about 55 iterations, the accuracy and training loss of the LSTM algorithm converged to stability, while the accuracy and training loss of the graph neural network converged to stability after about 30 iterations. Both during and after convergence, the graph neural network-based vulnerability detection algorithm had higher accuracy and smaller training loss.

2) For different types of vulnerabilities, the vulnerability detection algorithms had different performance, but overall, the graph neural network-based algorithm had the highest detection accuracy, followed by the LSTM algorithm, and the SVM algorithm had the lowest accuracy.

3) The SVM algorithm had the longest detection time, followed by LSTM, and the graph neural network algorithm consumed the least time.

References

[1] M. A. Albahar, "A modified maximal divergence sequential auto-encoder and time delay neural network models for vulnerable binary codes detection," *IEEE Access*, vol. 8, pp. 14999-15006, 2020.

[2] J. Gao, Y. Jiang, Z. Liu, X. Yang, C. Wang, X. Jiao, Z. Yang, J. Sun, "Semantic learning and emulation based cross-platform binary vulnerability seeker," *IEEE Transactions on Software Engineering*, vol. 47, no. 11, pp. 2575-2589, 2019.

[3] M. Ghaffarian, "Neural software vulnerability analysis using rich intermediate graph representations of programs," *Information Sciences: An International Journal*, vol. 553, no. 1, pp. 189-207, 2021.

[4] J. Hu, J. Chen, L. Zhang, Y. Liu, Q. Bao, H. Ackah-Arthur, C. Zhang, "A memory-related vulnerability detection approach based on vulnerability features," *Tsinghua Science and Technology*, vol. 25, no. 5, pp. 604-613, 2020.

[5] Y. Jiang, X. Su, C. Treude, T. Wang, "Hierarchical semantic-aware neural code representation," *Journal of Systems and Software*, vol. 191, pp. 1-21, 2022.

[6] Z. Li, D. Zou, J. Tang, Z. Zhang, M. Sun, H. Jin, "A comparative study of deep learning-based vulnerability detection system," *IEEE Access*, vol. 7, pp. 103184-103197, 2019.

Table 1: Detection performance and time consumption of three vulnerability detection algorithms for different vulnerability types

Algorithms	Performance Indicator	CWE-125	CWE-20	CWE-190	CWE-399	CWE-400
SVM	Precision	0.67	0.68	0.69	0.68	0.67
	Recall rate	0.59	0.58	0.59	0.58	0.58
	F-value	0.63	0.63	0.64	0.63	0.62
	Detection time/s	1.97	1.96	1.97	1.97	1.96
LSTM	Precision	0.87	0.88	0.86	0.87	0.88
	Recall rate	0.75	0.74	0.76	0.77	0.74
	F-value	0.81	0.80	0.81	0.82	0.80
	Detection time/s	1.12	1.11	1.10	1.12	1.10
Graph neural network	Precision	0.95	0.96	0.94	0.97	0.95
	Recall rate	0.87	0.86	0.87	0.85	0.86
	F-value	0.91	0.91	0.90	0.91	0.90
	Detection time/s	0.31	0.32	0.31	0.30	0.31

[7] H. Liang, Z. Xie, Y. Chen, H. Ning, J. Wang, "FIT: Inspect vulnerabilities in cross-architecture firmware by deep learning and bipartite matching," *Computers & Security*, vol. 99, no. 3-4, pp. 1-17, 2020.

[8] G. Tang, L. Yang, S. Ren, L. Meng, F. Yang, H. Wang, "An automatic source code vulnerability detection approach based on KELM," *Security and Communication Networks*, vol. 2021, no. 1, pp. 1-12, 2021.

[9] H. Wang, G. Ye, Z. Tang, S. H. Tan, S. Huang, D. Dang, Y. Feng, L. Bian, Z. Wang, "Combining graph-based learning with automated data collection for code vulnerability detection," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1943-1958, 2020.

[10] X. Wang, Q. Zheng, K. Zheng, Y. Sui, J. Zhang, "Semi-GSGCN: Social robot detection research with graph neural network," *Computers, Materials, and Continuum*, vol. 65, no. 1, pp. 617-638, 2020.

[11] Y. Wang, Z. Wu, Q. Wei, Q. Wang, "NeuFuzz: Efficient fuzzing with deep neural network," *IEEE Access*, vol. 7, pp. 36340-36352, 2019.

[12] L. Xie, D. Pi, X. Zhang, J. Chen, Y. Luo, W. Yu, "Graph neural network approach for anomaly detection," *Measurement*, vol. 180, no. 1, pp. 1-11, 2021.

[13] L. Yu, Y. Lu, Y. Shen, H. Huang, K. Zhu, "BE-Detector: A two-channel encoding method to detect vulnerabilities based on binary similarity," *IEEE Access*, vol. 9, pp. 51631-51645, 2021.

[14] M. Zhou, J. Chen, Y. Liu, H. Ackah-Arthur, S. Chen, Q. Zhang, Z. Zeng, "A method for software vulnerability detection based on improved control flow graph," *Journal of Natural Science of Wuhan University*, vol. 24, no. 2, pp. 149-160, 2019.

Biography

Lei Zhang was born in Hebei, China, she studied in Yunnan Normal University and received her bachelor's degree in 2008. Form 2010 to 2013 she studied in North China Electric Power University and received her Master's degree in 2013. She works in Baoding Vocational and Technical College, and she is mainly engaged in the research and teaching of network technology. She has obtained many honors such as Huawei HCIP certification, and has published many professional papers in national and provincial journals. She has applied for a number of software copyrights and patents.

Zehui Liu was born in Hebei, China, in 1974. From 2001 to 2005, he studied in Hebei Normal University and received his bachelor's degree in 2005. From 2014 to 2017, he studied in Tianjin Vocational and Technical Normal University and received his Master's degree in 2017. He is mainly engaged in the research of network security, computer technology, artificial intelligence, network technology and other related directions. He has obtained many honors such as HCNP certification, and has published many professional papers in national and provincial journals. He has applied for a number of software copyrights and patents.

Adaptive Salp Swarm Algorithm Based on Lens Imaging and Gaussian Mutation Learning Strategies

Junfu Xi[1], Yehua Chen[2], Xiaoji Chen[1], and Jun Li[1]
(Corresponding author: Jun Li)
Information Engineering Department, Hebei Vocational University of Technology and Engineering[1]
Xingtai, Hebei 054035, China
Email: beij-08@163.com
Accounting Department, Hebei Vocational University of Technology and Engineering[2]
Xingtai, Hebei 054035, China
(Received Oct. 31, 2022; Revised and Accepted May 12, 2023; First Online June 24, 2023)

Abstract

To overcome the slow convergence speed, decrease population diversity in later iterations, and low optimization accuracy of the standard Salp swarm algorithm (SSA), an adaptive Salp swarm algorithm (ASSA) based on lens imaging and Gaussian variation learning strategies is proposed. First, inspired by the particle swarm optimization algorithm, an adaptive attraction factor is designed and introduced into the follower position update to improve the ASSA's convergence speed and optimization accuracy. Then, based on lens imaging and Gaussian mutation, a learning strategy is designed to enhance the population diversity and improve the escape ability of the algorithm when it falls into a local optimum. Finally, seven typical algorithms are compared to optimize and simulate 14 benchmark test functions in different dimensions. The results show that ASSA's optimization accuracy, convergence speed, and stability significantly improve.

Keywords: Adaptive Multi-Factor Authentication; Gaussian Mutation Learning; Lens Imaging Learning; Salp Swarm Algorithm

1 Introduction

The swarm intelligence optimization algorithm is an emerging evolutionary computing technique that mimics the foraging and nesting behavior of animals and insects in nature. Compared with traditional optimization methods, it has better efficiency and stability in solving various complex optimization problems. In the past 20 years, many swarm intelligence optimization algorithms, such as particle swarm optimization (PSO) [26], whale optimization algorithm (WOA) [4], sine and cosine algorithm (SCA) [14], gray wolf optimization algorithm (GWO) [16], crisscross optimization algorithm (CSO) [13] and Bat Algorithm (BA) [24] have been proposed for solving complex global optimization problems [7, 22].

Salp Swarm Algorithm (SSA) is a new swarm intelligence optimization algorithm proposed by Mirjalili et al. in 2017. It originated from the simulation of the group foraging behavior of salps in the ocean. An effective optimization method was constructed through motion and chain following. SSA has been widely used in image segmentation [2], medical diagnosis [23], feature extraction [27], distribution network reconfiguration [1] and global numerical optimization [21] due to its simple principle and few control parameters [15]. However, similar to other swarm intelligence optimization algorithms, it still has disadvantages of low solution accuracy, slow convergence speed and easy to fall into the local optimum. To overcome these shortcomings, many improved SSA algorithms based on different strategies has been proposed. Liu et al. introduced the inertia weight coefficient to modify the leader position update formula. An adaptive adjustment strategy in the selection of global and local search was introduced to improve the optimization accuracy and stability of the algorithm [11]. The predator-prey strategy in Harris Hawk algorithm is integrated into the position update equation of the follower to maintain the balance between the global and local search of the algorithm [19]. To modify the position update formulas of leaders and followers, Fan et al. introduced a perturbation weight mechanism to improve the convergence speed, and balance the exploration and development capabilities of the algorithm [6]. Ibrahim et al. designed the SSAPSO (a hybrid optimization algorithm of SSA and PSO). It compares random numbers with fixed values to select a search strategy, improving the global development and local exploration capabilities of the algorithm [9]. Abd et al. designed the SSDE (a hybrid optimization algorithm

of SSA and DE). This algorithm used the operator of the differential evolution algorithm as a local search operator to enhance the feature mining ability of the algorithm [5]. Ren et al. introduced adaptive weights and Levy flight operator into SSA to balance the global and local search capabilities of the algorithm [20]. Zhang et al. introduced a pure initialization and differential evolution mechanism to improve the convergence speed and accuracy of the algorithm [25]. Besides this, Panda and Majhi introduced a normal distribution mutation operator and an adversarial learning strategy to improve the exploration and development capabilities in the search area of the algorithm [18].

The above researches has improved the standard SSA and enhanced the performance of the algorithm, but there are still some shortcomings:

1) The improved search strategy ignores that the algorithm should adopt different learning strategies under divergence and aggregation behaviors. It will reduce the population diversity and may still fall into the local optimum when dealing with high-dimensional complex problems.

2) In the current improvement to the follower position update formula, the position of the global optimal individuals is not well utilized, and the convergence speed and solution accuracy are not significantly improved.

To overcome the above defects, an adaptive salp swarm algorithm (ASSA) based on lens imaging and gaussian mutation learning strategy is proposed. It uses lens imaging and gaussian mutation learning strategy to improve the learning ability of the algorithm, increase the diversity of the population and jump out of the local optimum. The follower position update is guided by an adaptive attraction factor to improve the convergence speed and solution accuracy. To verify the optimization performance of the algorithm, 14 benchmark functions are tested and analyzed by ASSA, PSO, GWO, WOA, SCA and ISSA and the effectiveness of ASSA is verified. The main contributions of the paper are as follows:

1) To improve the escape ability of the local optimum of the algorithm, a learning strategy that combines lens imaging and Gaussian mutation is proposed;

2) An adaptive attraction factor is designed to improve the solution accuracy and convergence speed of the algorithm;

3) The effectiveness of ASSA is verified.

The following sections are arranged as: Section 2 introduces the standard salp swarm algorithm; Section 3 introduces and analyzes the ASSA algorithm; Section 4 shows the experimental parameters, experimental environment and effectiveness verification of the ASSA, and Section 5 draws the conclusion.

2 Salp Swarm Algorithm

The salp swarm algorithm simulates the individual connection of the salp group in foraging. Its purpose is to form the leaders and followers in the salp chain to cooperate with each other for search optimization. The front end of the salp chain is the leaders, responsible for leading the entire population to explore the position of food source in the search space. The rest individuals are the followers, following the leaders to conduct local searches.

In SSA, assuming that N salps are in the D-dimensional search space, the position of each salp is:

$$X = \begin{bmatrix} x_1^1 & x_1^2 & \cdots & x_1^j & \cdots & x_1^D \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ x_i^1 & x_i^2 & \cdots & x_i^j & \cdots & x_i^D \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ x_N^1 & x_N^2 & \cdots & x_N^j & \cdots & x_N^D \end{bmatrix}$$

where $i = 1, 2, \ldots, N$, $j = 1, 2, \ldots, D$, x_i^j represents the position of the i^{th} salp in the j^{th} dimension.

The leaders guide the movement of the entire salp population and conduct a random search guided by the current food source. Its position update equation is as follows:

$$x_1^j = \begin{cases} F_j + c_1((ub_j - lb_j)c_2 + lb_j), & c_3 \geq 0.5 \\ F_j - c_1((ub_j - lb_j)c_2 + lb_j), & c_3 < 0.5 \end{cases} \quad (1)$$

where x_1^j is the position of leaders in the j^{th}-dimensional search space; F_j is the position of the food source in the j^{th}-dimensional search space; ub_j and lb_j are the upper and lower bounds of the j^{th}-dimensional search space, respectively; c_2 and c_3 are random numbers uniformly distributed in $[0, 1]$; c_1 is the control factor, which controls the search method of the algorithm at different stages. The calculation formula is:

$$c_1 = 2e^{-(4t/T)^2} \quad (2)$$

where t is the number of iterations in the current algorithm, and T is the maximum number of iterations set by the algorithm.

When the position of leaders is updated, the followers follow and move in a chain, and the position update formula is:

$$x_i^j = \frac{1}{2}(x_i^j + x_{i-1}^j) \quad (3)$$

where x_i^j is the position of the i^{th} follower in the j^{th} dimensional search space, and $i \geq 2$.

3 Improved ASSA

3.1 Adaptive Attraction Factor

In the iterative optimization process of SSA, as shown in Formula (3), the position of the i^{th} salp will be updated

according to the midpoint of the historical position of the $i-1^{\text{th}}$ and i^{th} salps. This single following behavior just uniaxially accepts the position information of the former to update the current position. When the leaders in the population fall into the local optimum, the followers will inevitably fall into the local optimum. This will lead to the premature convergence of the algorithm and limit the search efficiency to a certain extent [3].

At each iteration of the particle swarm algorithm, each particle will accelerate toward its own optimal solution. It will also continuously search for the optimal solution towards the global optimal position found so far by any particle in the population. In this way, an adaptively adjusted attraction factor c_4 is introduced based on the global optimal position distribution of the population in D-dimension. Substituting the attraction factor c_4 into the position of the followers to update the formula, the new formula is as follows:

$$x_i^j = \frac{c_4}{2}(x_i^j + x_{i-1}^j) \tag{4}$$

$$c_4 = (p_b - p_s)/t,\ t \neq 0 \tag{5}$$

where, c_4 is the attraction factor with the initial value of 1; p_b and p_s are the maximum and minimum values in the D-dimension of the historical optimal position of the population at the t^{th} iteration.

Several different types of benchmark functions are experimented. Due to space limitations, Figure 1 is the attraction factor curves of the three benchmark functions (Sphere, Alpine and Easom) solved by SSA with adaptive attraction factors. Sphere is a unimodal function; Alpine is a multimodal function, and the function dimension is set to $D = 30$. Easom is a fixed $D = 2$ dimensional function; the population size $N = 30$, and the maximum number of iterations is $T = 500$.

Compared with Formula (3), Formula (4) has the following characteristics: It can be seen from Figure 1 that in the early stage of iteration, the attraction factor obtains a larger value, which is conducive to the global development of the algorithm and can accelerate the convergence speed. As the iterations increase, the attraction factor gradually decreases and tends to 0. This is beneficial to the algorithm to carry out local exploration and improve the algorithm convergence accuracy in the late stage of iteration. Since the followers are attracted by the global optimal position of the current population, an adaptive update is generated to improve the ability of the algorithm to jump out of the local optimum.

3.2 Lens Imaging and Gaussian Mutation Learning Strategies

In the iterative search process of SSA, the global optimal position of the population is updated with the position of individuals with the best fitness value. While the position adjustment of the optimal and other non-optimal individual is ignored. This leads to a gradual decrease in population diversity and may lead to SSA falling into local optimum. In order to increase the probability of SSA to improve the optimization accuracy and jump out of the local optimum, lens imaging and Gaussian mutation learning strategies are introduced. According to the phenomenon of "divergence" or "aggregation" in the current population, the lens imaging or Gaussian mutation learning strategy is used to mutate individuals to increase the population diversity.

3.2.1 Lens Imaging Learning Strategy

Lens image based learning strategy (LIBLS) is a new learning strategy that uses the principle of lens imaging and combined with reverse learning strategy to find better candidate solutions. This strategy cannot only strengthen the group diversity, but also improve the ability to jump out of local optimum and improve the global search ability [12, 17]. The basic principle of LIBLS is shown in Figure 2.

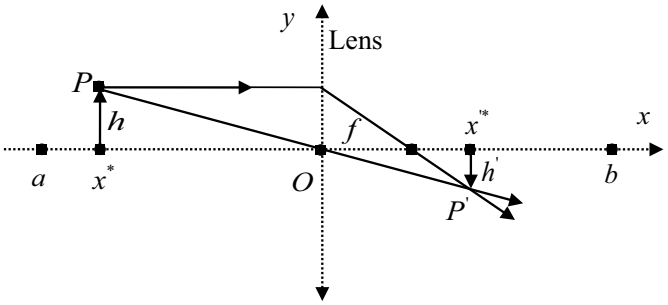


Figure 2: Schematic diagram of the lens imaging strategy

In Figure 2, taking one-dimensional space as an example, the search interval for the solution on the axis x is $[a, b]$; y-axis is the normal; the base point O is the midpoint in $[a, b]$; x^* represents the projection of an individual P with height h on the coordinate axis in space, which is the global optimal individual; f is the focal length of the lens placed at the base position O; x'^* is the projection of an image P' with height h' on the coordinate axis obtained by the lens imaging in space, which is a new individual generated by a reverse learning strategy based on the lens imaging principle. From the lens imaging principle, we can obtain:

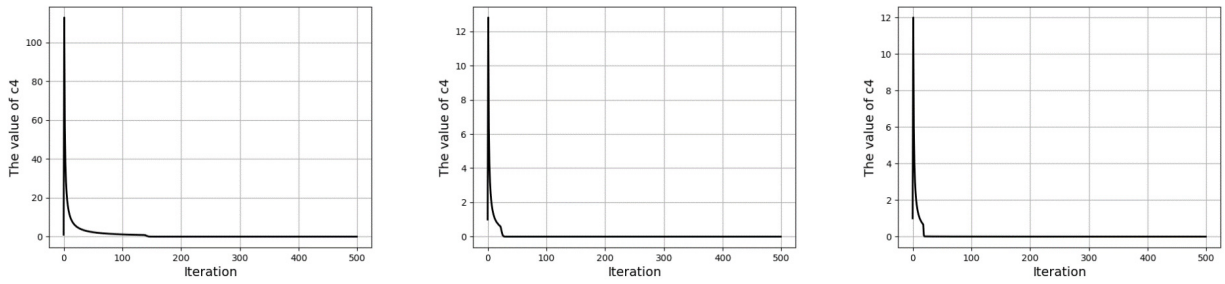
$$\frac{\frac{a+b}{2} - x^*}{x'^* - \frac{a+b}{2}} = \frac{h}{h'} \tag{6}$$

Let $h/h' = k$, k is the adjustment factor, and Formula (6) is transformed to obtain the calculation formula of the lens imaging reverse learning solution:

$$x'^* = \frac{a+b}{2} + \frac{a+b}{2k} - \frac{x^*}{k} \tag{7}$$

When $k = 1$ and $n = 1$, Formula (7) can be transformed into the standard reverse learning solution:

$$x'^* = a + b - x^* \tag{8}$$



(a) Sphere function (b) Alpine function (c) Easom function

Figure 1: Curves of the attract factor c_4

From Formulas (7) and (8), the reverse learning strategy is only a special case of LIBLS. LIBLS can obtain a dynamic new candidate solution by adjusting the parameter k to enhance the population diversity.

Formula (7) is extended to the D-dimensional space based on LIBLS to obtain Formula (9):

$$x_j'^* = \frac{a_j + b_j}{2} + \frac{a_j + b_j}{2k} - \frac{x_j^*}{k} \tag{9}$$

where x_j^x and $x_j'^*$ are the j^{th}-dimensional components of x^* and x'^*, respectively; a_j and b_j are the j^{th}-dimensional components of the upper and lower boundaries of the decision variable, respectively.

3.2.2 Gaussian Variation Learning Strategy

The image of the probability density function of Gaussian mutation about the expectation is symmetrical. About 99.8% of the area in the function curve is within the range of three times the standard deviation of the expectation. That is, the random numbers obtained are concentrated in the local area centered on the expectation [10]. As such, the key search area of Gaussian mutation is a local area near the salps and it has strong local search ability, high efficiency, high precision and robustness. The formula for Gaussian mutation learning strategy is as follows:

$$x'^* = x^*(1 + N(0,1)) \tag{10}$$

where x^* and x'^* are the positions before and after individual variation, and $N(0,1)$ is a standard normal distribution with an expected value of 0 and a variance of 1.

3.3 ASSA Pseudocode

The pseudocode of ASSA is shown in Algorithm 1.

Algorithm 1 ASSA

Input: The population size N, the adjustment factor k; the dimension of the objective function D; the search boundary $[lb, ub]$, the maximum number of interaction T or the solution accuracy ε;

Output: The optimal position F_d, and the optimal function value F_g.

Generate N D-dimensional vectors in the search range. The individual fitness value of each salp and the average fitness value f_{avg} of the salp population are calculated to sort the fitness values, let = 1.
while $t < T$ **do**
  Update according to Formula (2);

$$c_2 \in [0,1];$$
$$c_3 \in [0,1];$$

  Update c_4 according to Formula (5);
  for $i = 1 : N$ **do**
    if $i = 1 : N/2$ **then**
      Update the leader position by Formula (1);
    else
      Update the follower position by Formula (4);
    end if
    Calculate the fitness value$f_i$of each salp
    if $f_i < f_{avg}$ **then**
      According to Formula (10), Gaussian mutation learningis carried out to correct the boundary. If the individual after mutation is better than the individual before mutation, corresponding replacement is made; otherwise, do not replace;
    else
      According to Formula (9), lens imaging learning is carried out to correct the boundary. If the individuals after mutation are better than the individual before mutation, corresponding replacement is made; otherwise, do not replace;
    end if
  end for
  Update the optimal position F_d of the contemporary population, optimal fitness value F_g and the average fitness value f_{avg};
  $t = t + 1$
end while
return to F_d, F_g

3.4 Time Complexity Analysis

Assuming that the population size of the algorithm is N; the dimension of the objective function is D; the maximum number of iterations is T, and the calculation amount of the objective function of the optimization problem is C. According to the operation rules of time complexity, the time complexity of standard SSA is $O(T \cdot (N \cdot D + N \cdot C))$ [15].

From Algorithm 1, the adjustment of the adaptive attraction factor c_4, the optimal and non-optimal individual positions are the steps added by the ASSA. According to the time complexity operation rules, in one iteration, the time complexity corresponding to the added steps are $O(1)$ and $O(N)$. In T iterations, the time complexity increased by ASSA is $O(T \cdot (1+N))$, and the order of magnitudes of the algorithm is not improved. In this way, the time complexity of ASSA is still $O(T \cdot (N \cdot D + N \cdot C))$, indicating that the calculation of ASSA does not increase too much.

4 Experiment and Analysis

4.1 Test Function and Parameter Setting

To verify the optimization performance of ASSA, simulation experiments are carried out on 14 typical benchmark functions using PSO, GWO, WOA, SCA, ISSA [8] and ASSA. The specific parameter s of each algorithm are shown in Table 1, and the benchmark functions are shown in Table 2. $F_1 \sim F_6$ are the high-dimensional unimodal functions; $F_7 \sim F_{12}$ are the high-dimensional multimodal functions; F_{13} and F_{14} are the fixed dimension functions ($D = 2$). The simulation experiments are performed on Intel(R) Core(TM) i7-9700 CPU@3.00GHz, 16GB RAM, Windows 10 64-bit operating system with Python 3.9.1

4.2 Optimization Accuracy and Stability Analysis

To test the optimization performance of ASSA, the dimensions of the benchmark functions f_1-f_{12} are set to 30, 50, 100, respectively, and that of f_{13} and f_{14} are $D = 2$. The population size and maximum number of iterations for each algorithm are set to 30 and 500, respectively. To compare the fairness and objectivity of the experiments, the seven algorithms independently run for 30 times under the same conditions. Their optimal value (*Best*), average value (*Ave*) and standard deviation (*Std*) are taken as the evaluation indicators. The optimal results after optimization are in bold (Table 3).

The optimization accuracy and stability of the proposed ASSA are analyzed through the three dimensions of the tested unimodal function, multimodal function and fixed dimension function.

1) For the unimodal functions $F_1 \sim F_6$, when $D = 30$, the optimal value (*Best*), average value (*Ave*) and standard deviation (*Std*) of the optimization results of the seven algorithms on the functions F_1, F_2, F_3 and F_4 show that, ASSA reaches the theoretical optimal value of 0, and the other 6 algorithms do not. The solution accuracy of ASSA is much higher than that of the other 6 algorithms. For the function F_5, ASSA has the highest solution accuracy, reaching the exponential level of 1e-07, followed by the GWO algorithm with an exponential level of 1e+01. The *Ave* and *Std* of the ASSA optimization results are higher than the other 6 algorithms. For the function F_6, ASSA has the highest solution accuracy, reaching the exponential level of 1e-07, followed by ISSA with an exponential level of 1e-05. The *Ave* and *Std* of the ASSA and ISSA optimization results are on the same exponential level.

   When $D = 50$ and $D = 100$, the *Best*, *Ave* and *Std* of ASSA on the functions F_1, F_2, F_3 and F_4 still reach the theoretical optimal value of 0. The other 6 algorithms not only fail to reach the theoretical optimal value, but also reduce the optimization performance as the dimension increases. For the functions F_5 and F_6, ASSA has the highest solution accuracy, reaching the exponential level of 1e-06, followed by the 1e+01 and 1e-04 exponential levels of ISSA. The *Ave* and *Std* of the ASSA optimization results are better than the other 6 algorithms.

2) For the multimodal functions $F_7 \sim F_{12}$, when $D = 30$, the *Best*, *Ave* and *Std* of the seven algorithms on the functions F_7, F_{10} and F_{11} show that, ASSA has reached the theoretical optimal value of 0, and the other 6 algorithms do not reach. The solution accuracy of ASSA is much higher than that of the other 6 algorithms. For the function F_9, the optimal values of ASSA, WOA and GWO all reach the theoretical optimal value of 0, and the *Ave* and *Std* optimized by ASSA and GWO also reach the theoretical optimal value of 0. For the function F_8, ASSA has the highest solution accuracy, reaching the exponential level of 1e-16. *Std* is 0, followed by the exponential level of 1e-14 of GWO. The *Ave* and *Std* of the ASSA optimization result are higher than the other 6 algorithms.

   When $D = 50$ and $D = 100$, the *Best*, *Ave* and *Std* of ASSA on the functions F_7, F_{10} and F_{11} reach the theoretical value of 0, and the other 6 algorithms do not reach. The solution accuracy of ASSA is higher than the other 6 algorithms. For the function F_9, ASSA has the optimal optimization results, and its *Best*, *Ave* and *Std* reach the theoretical optimal value of 0. Followed is GWO, whose *Best*, *Ave* and *Std* reach the theoretical optimal value of 0 when $D = 50$. Its optimization accuracy can only reach the exponential level of 1e-14 in the $D = 100$ dimension. For the functions F_8 and F_{12}, ASSA still has the highest solution accuracy, reaching the exponential level of 1e-16, 1e-16 and 1e-07, 1e-06, respectively, followed

Table 1: Parameters

Algorithm	PSO	GWO	WOA	SCA	ISSA	ASSA
Parameter	$c_1 = 2$, $c_2 = 2$, $W_{\min} = 0.2$, $W_{\max} = 0.9$	$a = (2 \to 0)$	$b = 1$	$r_2 \in [0, 2\pi]$, $a = 2$, $r_3 \in [-2, 2]$, $r_4 \in [0, 1]$	$w = 0.7$	$K = 12000$

Table 2: Test functions

Function	Formula	Domain	Min
Sphere	$F_1(x) = \sum_{i=1}^{n} x_i^2$	$[-100, 100]$	0
Schwefel's 2.22	$F_2(x) = \sum_{i=1}^{n} \lvert x_i \rvert + \prod_{i=1}^{n} \lvert x_i \rvert$	$[-10, 10]$	0
Quadric	$F_3(x) = \sum_{i=1}^{n} \sum_{j=1}^{i} x_j^2$	$[-100, 100]$	0
Schwefel's 2.21	$F_4(x) = \max_i \{\lvert x_i \rvert, 1 \le i \le n\}$	$[-100, 100]$	0
Rosenbrock	$F_5(x) = \sum_{i=1}^{n-1} [100(x_{i+1} - x_i^2)^2 + (x_i - 1)^2]$	$[-30, 30]$	0
Quartic	$F_6(x) = \sum_{i=1}^{n} i x_i^4 + \text{random}[0, 1]$	$[-1.28, 1.28]$	0
Rastrigin	$F_7(x) = \sum_{i=1}^{n} [x_i^2 - 10\cos(2\pi x_i) + 10]$	$[-5.12, 5.12]$	0
Ackley	$F_8(x) = -20\exp\left(-0.2\sqrt{\frac{1}{n}\sum_{i=1}^{n} x_i^2}\right) - \exp\left(\frac{1}{n}\sum_{i=1}^{n}\cos(2\pi x_i)\right) + 20 + e$	$[-32, 32]$	0
Griewank	$F_9(x) = \frac{1}{4000}\sum_{i=1}^{n} x_i^2 - \prod_{i=1}^{n}\cos\left(\frac{x_i}{\sqrt{i}}\right) + 1$	$[-600, 600]$	0
Zakharov	$F_{10}(x) = \sum_{i=1}^{n} x_i^2 + \left(\sum_{i=1}^{n} 0.5 i x_i\right)^2 + \left(\sum_{i=1}^{n} 0.5 i x_i\right)^4$	$[-5, 10]$	0
Alpine	$F_{11}(x) = \sum_{i=1}^{n} \lvert x_i \sin(x_i) + 0.1 x_i \rvert$	$[-10, 10]$	0
Generalized Penalized	$F_{12}(x) = 0.1\{\sin^2(3\pi x_1) + \sum_{i=1}^{n-1}(x_i - 1)^2[1 + \sin^2(3\pi x_{i+1})] + (x_n - 1)[1 + \sin^2(2\pi x_n)]\} + \sum_{i=1}^{n} u(x_i, 5, 100, 4)$	$[-50, 50]$	0
Easom	$F_{13}(x) = -\cos(x_1)\cos(x_2)\exp(-(x_1 - \pi)^2 - (x_2 - \pi)^2)$	$[-100, 100]$	-1
Six-Hump Camel	$F_{14}(x) = 4x_1^2 - 2.1x_1^4 + \frac{1}{3}x_1^6 + x_1 x_2 - 4x_2^2 + 4x_2^4$	$[-5, 5]$	-1.0316

by e-12, 1e-12 of GWO and 1e-03 and 1e+0 of ISSA. The *Ave* and *Std* of the ASSA optimization results are better than the other 6 algorithms.

3) For the fixed dimensional functions $F_{13} \sim F_{14}$, in the $D = 2$ dimension, the *Best*, *Ave* and *Std* of the optimal results of ASSA and PSO algorithms on the functions all reach the theoretical optimal value, slightly better than the other 5 algorithms. The *Best* and *Ave* of the optimal results of ASSA, SSA, WOA and PSO algorithms on the functions all reach the theoretical optimal value, and PSO has the best stability.

ASSA shows better solution performance when solving different dimensions of unimodal and multimodal benchmark functions. Its solution accuracy and stability in $D = 10$, 50, and 100 dimensions are obviously better than those of the other six algorithms. ASSA also shows better optimization accuracy and stability when solving the benchmark function with the fixed dimension $D = 2$.

4.3 Convergence Curve Analysis

To reflect the dynamic convergence characteristics of ASSA, Figure 3 shows the convergence curves of 7 optimization algorithms for 14 benchmark functions under $D = 50$.

For the functions F_1, F_2, F_3, F_4, F_7, F_9, F_{10}, F_{11}, F_{13} and F_{14}, ASSA is obviously superior to the other 6 algorithms in convergence speed and optimization accuracy. It can optimize with the minimum number of iterations. For the functions F_5, F_6 and F_{12}, From Figure 3(e), 3(f) and 3(l), ASSA quickly falls into the local optimum in the early stage of the iteration, but continues to jump out of the local optimum as the iteration progresses and continues to search. Its search accuracy is higher than the other 6 algorithms. For the function F_8, it can be seen from Figure 3(h) that ASSA converges rapidly in the early stage of the iteration, but quickly falls into the local extreme value and cannot escape. At the end of the iteration, the accuracy of the other six algorithms is still far lower than the optimization accuracy of ASSA.

As shown in Figure 3, ASSA can greatly improve the iterative speed and search ability of the standard SSA algorithm. This is mainly because the adaptive attraction factor is introduced in the follower position update, which enables the algorithm to converge quickly while improving the search ability and stability. The lens imaging and Gaussian mutation learning strategies are introduced to enhance the population diversity, so that the algorithm can effectively jump out of the local optimum and improve the ability of the algorithm to avoid falling into the local optimum.

Table 3: Optimization performance comparison of the seven algorithms

Functions	Algorithms	$D = 30$			$D = 50$			$D = 100$		
		Best	Ave	Std	Best	Ave	Std	Best	Ave	Std
$F_1(x)$	SSA	1.79E+01	3.12E+01	1.87E+01	9.23E+02	1.93E+03	1.42E+03	5.20E+04	5.56E+04	4.96E+03
	ASSA	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
	ISSA	2.52E-09	2.84E-09	3.58E-10	5.02E-09	5.03E-09	1.28E-11	1.09E-08	1.14E-08	7.47E-10
	WOA	6.34E-22	7.62E-20	1.06E-19	6.52E-19	3.24E-16	4.57E-16	2.49E-13	1.92E-12	2.37E-12
	GWO	9.96E-32	1.79E-31	1.12E-31	6.49E-23	1.45E-22	1.14E-22	4.96E-15	2.48E-14	2.81E-14
	PSO	8.79E-01	1.056693	2.51E-01	1.24E+01	1.31E+01	9.01E-01	9.13E+01	1.03E+02	1.77E+01
	SCA	5.41E-01	1.428195	1.254190	4.48E+02	5.04E+02	7.93E+01	5.49E+03	1.04E+04	6.97E+03
$F_2(x)$	SSA	8.73E+01	9.76E+01	1.45E+01	1.57E+02	1.59E+02	2.959858	1.29E+21	1.02E+25	1.45E+25
	ASSA	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
	ISSA	1.88E-05	2.18E-05	4.24E-06	3.69E-05	3.95E-05	3.66E-06	7.85E-05	8.41E-05	7.88E-06
	WOA	1.18E-15	2.27E-14	3.04E-14	4.46E-12	1.21E-11	1.08E-11	1.01E-08	1.18E-08	2.43E-09
	GWO	6.70E-19	1.07E-18	5.72E-19	1.19E-13	1.42E-13	3.24E-14	5.39E-09	6.21E-09	1.14E-09
	PSO	3.530267	4.765212	1.746476	1.07E+01	1.25E+01	2.637469	5.21E+01	5.32E+01	1.223561
	SCA	1.24E-03	1.12E-02	1.37E-02	4.13E-02	2.13E-01	2.43E-01	3.747045	1.46E+01	1.54E+01
$F_3(x)$	SSA	1.27E+04	1.28E+04	1.77E+02	4.55E+04	5.21E+04	9.23E+03	1.60E+05	1.85E+05	3.50E+04
	ASSA	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
	ISSA	6.07E-09	6.26E-09	2.79E-10	1.86E-08	2.39E-08	7.93E-08	7.93E-08	1.11E-07	4.57E-08
	WOA	6.25E-04	8.86E-03	1.16E-02	2.44E-02	4.32E-02	2.26E-02	6.564214	5.69E+01	3.94E+01
	GWO	6.04E-08	1.74E-05	2.45E-05	1.31E-04	5.16E-03	7.11E-03	2.32E+02	4.65E+02	3.28E+02
	PSO	3.53E+01	1.10E+02	1.06E+02	9.99E+02	1.33E+03	4.67E+02	1.11E+04	4.12E+04	4.25E+04
	SCA	7.90E+03	8.04E+03	1.33E+02	3.63E+04	4.87E+04	1.76E+04	1.97E+05	2.10E+05	1.95E+04
$F_4(x)$	SSA	5.09E+01	5.38E+01	4.063068	6.28E+01	6.28E+01	5.90E-02	6.81E+01	7.01E+01	2.957833
	ASSA	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
	ISSA	1.72E-05	1.77E-05	7.01E-07	2.09E-05	2.14E-05	7.07E-07	1.82E-05	2.17E-05	4.87E-06
	WOA	1.76E-04	2.22E-04	6.46E-05	2.52E-04	2.32E-03	2.92E-03	5.83E-03	9.76E-03	5.56E-03
	GWO	4.70E-07	4.82E-07	1.68E-08	1.48E-04	2.88E-04	1.98E-04	2.39E-01	3.14E-01	1.06E-01
	PSO	3.509552	4.312612	1.135698	6.953711	7.301870	4.92E-01	1.01E+01	1.05E+01	7.02E-01
	SCA	4.15E+01	4.37E+01	3.120831	4.63E+01	5.46E+01	1.71E+01	8.52E+01	8.73E+01	2.915663
$F_5(x)$	SSA	1.83E+04	4.03E+04	3.11E+04	3.44E+06	4.29E+06	1.20E+06	7.67E+07	1.04E+08	3.96E+07
	ASSA	**2.60E-07**	**1.37E-02**	**1.94E-02**	**7.17E-06**	**1.15E-05**	**6.24E-06**	**8.79E-06**	**1.47E-05**	**8.40E-06**
	ISSA	2.88E+01	2.85E+01	7.94E-02	3.81E+01	2.88E+01	4.61E-01	5.87E+01	4.88E+01	1.07E-01
	WOA	2.85E+01	2.86E+01	1.69E-01	4.79E+01	4.82E+01	5.55E-01	9.84E+01	9.69E+01	1.65E-02
	GWO	2.71E+01	2.75E+01	5.52E-01	4.60E+01	4.73E+01	1.814418	9.68E+01	9.69E+01	1.01E-01
	PSO	1.93E+02	2.02E+02	1.19E+01	1.34E+03	1.35E+03	1.07E+01	2.14E+04	2.28E+04	1.96E+03
	SCA	4.83E+03	7.10E+03	3.21E+03	1.89E+06	2.40E+06	7.15E+05	2.28E+07	1.31E+08	1.10E+08
$F_6(x)$	SSA	7.29E-01	7.33E-01	6.52E-03	5.355531	6.367908	1.771590	7.79E+01	1.08E+02	4.33E+01
	ASSA	**2.70E-07**	**1.67E-05**	**2.33E-05**	**4.04E-06**	**2.43E-05**	**2.87E-05**	**4.57E-06**	**2.45E-05**	**2.82E-05**
	ISSA	5.55E-05	8.98E-05	4.85E-05	1.26E-04	2.42E-04	1.63E-04	1.13E-04	2.89E-04	1.06E-04
	WOA	4.31E-04	8.70E-04	6.19E-04	6.49E-04	1.23E-03	8.26E-04	4.38E-04	6.27E-04	2.66E-04
	GWO	1.52E-03	1.84E-03	4.54E-04	3.38E-03	3.97E-03	8.35E-04	3.99E-03	7.00E-03	4.25E-03
	PSO	1.17E-01	1.34E-01	2.41E-02	1.186474	1.402419	3.05E-01	6.000036	8.381061	3.367271
	SCA	9.99E-02	1.26E-01	3.79E-02	8.55E-01	9.07E-01	7.38E-02	6.33E+01	1.07E+02	6.22E+01
$F_7(x)$	SSA	1.92E+02	2.02E+02	1.42E+01	3.78E+02	3.89E+02	1.57E+01	1.01E+03	1.01E+03	1.258601
	ASSA	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
	ISSA	1.26E-09	1.55E-09	4.02E-10	2.41E-09	2.77E-09	5.11E-10	5.36E-09	5.54E-09	2.53E-10
	WOA	5.68E-14	8.52E-14	4.01E-14	3.41E-13	3.41E-13	**0**	2.27E-13	4.54E-13	3.21E-13
	GWO	1.13E-13	2.713627	3.837648	2.67E-12	2.028241	2.868367	4.074922	1.31E+01	1.28E+01
	PSO	4.81E+01	6.13E+01	1.86E+01	1.55E+02	1.75E+02	2.85E+01	4.61E+02	5.27E+02	9.30E+01
	SCA	7.538779	2.51E+01	1.98E+01	1.67E+02	1.73E+02	8.453702	1.23E+02	1.97E+02	1.04E+02
$F_8(x)$	SSA	1.04E+01	1.45E+01	5.822159	1.66E+01	1.79E+01	1.836778	1.66E+01	1.79E+01	1.836778
	ASSA	**4.44E-16**	**4.44E-16**	**0**	**4.44E-16**	**4.44E-16**	**0**	**4.44E-16**	**4.44E-16**	**0**
	ISSA	1.22E-05	1.25E-05	3.60E-07	1.32E-05	1.37E-05	5.91E-07	1.32E-05	1.37E-05	5.91E-07
	WOA	4.91E-11	6.26E-11	1.89E-11	6.68E-10	7.34E-09	9.44E-09	6.68E-10	7.34E-09	9.44E-09
	GWO	5.01E-14	5.72E-14	1.04E-14	6.32E-13	1.36E-12	1.03E-12	6.32E-13	1.36E-12	1.03E-12
	PSO	5.014531	5.019510	7.04E-03	6.164623	6.651855	6.89E-01	6.164623	6.651855	6.89E-01
	SCA	2.02E+01	2.06E+01	1.97E-02	5.350508	1.28E+01	1.05E+01	5.350508	1.28E+01	1.05E+01

$F_9(x)$	SSA	6.98E-01	9.33E-01	3.32E-01	1.90E+01	6.22E+01	6.11E+01	5.76E+02	5.98E+02	3.02E+01
	ASSA	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
	ISSA	4.93E-09	5.12E-09	2.66E-10	5.35E-09	5.67E-09	4.59E-10	7.74E-09	8.28E-09	7.66E-10
	WOA	**0**	5.55E-17	7.85-17	8.88E-16	5.21E-15	6.12E-15	2.55E-13	4.61E-13	2.91E-13
	GWO	**0**	**0**	**0**	**0**	**0**	**0**	1.85E-14	2.39E-14	7.61E-15
	PSO	2.45E+01	2.83E+01	5.335829	4.43E+01	5.28E+01	1.20E+01	1.09E+02	1.18E+02	1.39E+01
	SCA	1.077995	1.092398	2.03E-02	2.098198	7.289237	7.341238	3.63E+01	3.94E+01	4.434841
$F_{10}(x)$	SSA	3.08E+02	3.34E+02	3.66E+01	5.41E+02	6.24E+02	1.16E+02	1.32E+03	1.61E+03	4.13E+02
	ASSA	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
	ISSA	4.46E-11	4.47E-11	1.49E-13	7.76E-11	1.09E-10	4.55E-11	2.57E-10	2.71E-10	1.96E-11
	WOA	8.80E-04	2.31E-03	2.03E-03	1.05E+01	3.21E+01	3.12E+01	8.724579	2.58E+01	2.41E+01
	GWO	1.39E-09	8.89E-09	1.06E-08	4.47E-03	2.35E-02	2.69E-02	8.81E+01	8.82E+01	7.97E-02
	PSO	5.33E+02	6.14E+02	1.14E+02	1.88E+03	2.38E+03	7.15E+02	1.30E+04	1.77E+04	6.73E+03
	SCA	4.534067	1.46E+01	1.43E+01	1.52E+02	1.76E+02	3.44E+01	8.03E+02	8.49E+02	6.60E+01
$F_{11}(x)$	SSA	1.06E+01	1.34E+01	3.901388	4.56E+01	4.76E+01	2.708009	1.16E+02	1.19E+02	4.793367
	ASSA	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
	ISSA	2.26E-06	2.27E-06	2.29E-08	4.17E-06	4.20E-06	3.33E-08	7.94E-06	8.23E-06	4.05E-07
	WOA	1.37E-14	2.13E-13	2.83E-13	6.52E-11	8.84E-11	3.28E-11	6.30E-10	2.02E-09	1.97E-09
	GWO	8.10E-04	1.27E-03	6.58E-04	1.94E-12	1.83E-04	2.58E-04	2.12E-08	1.84E-04	2.60E-04
	PSO	1.613568	2.078068	6.56E-01	7.162391	7.203426	5.80E+02	2.74E+01	3.24E+01	7.081835
	SCA	3.35E-02	4.85E-02	2.12E-02	6.687247	7.593677	1.281886	2.64E+01	3.13E+01	6.901256
$F_{12}(x)$	SSA	4.25E+01	2.20E+02	2.51E+02	1.40E+03	1.51E+03	1.55E+02	3.78E+03	3.86E+03	1.24E+02
	ASSA	**3.46E-08**	**4.75E-07**	**6.24E-07**	**9.94E-08**	**1.30E-07**	**4.36E-08**	**9.17E-07**	**1.38E-06**	**6.67E-07**
	ISSA	2.471437	2.629361	2.23E-01	4.786443	4.787930	2.10E-03	9.784981	9.785347	5.17E-04
	WOA	1.097028	1.255197	2.23E-01	3.109606	3.231111	1.71E-01	7.519092	8.035726	7.31E-01
	GWO	3.19E-01	3.64E-01	6.43E-02	1.541139	1.599278	8.22E-02	5.521556	5.867553	4.89E-01
	PSO	1.812416	2.502407	9.75E-01	2.51E+01	3.37E+01	1.21E+01	8.25E+01	1.03E+02	2.94E+01
	SCA	2.363502	2.369559	8.5E-03	4.820162	9.812401	7.060104	6.32E+01	2.67E+02	2.88E+02

$D = 2$

Function	Algorithms	Best	Ave	Std		Function	Algorithms	Best	Ave	Std
$F_{13}(x)$	SSA	-0.999999	-0.999999	5.07E-12		$F_{14}(x)$	SSA	**-1.031628**	**-1.031628**	2.08-14
	ASSA	**-1.0**	**-1.0**	**0**			ASSA	**-1.031628**	**-1.031628**	3.62-16
	ISSA	-0.993713	-0.993355	5.05E-04			ISSA	-1.031162	-1.027854	4.67E-04
	WOA	-0.999999	-0.999999	6.97E-07			WOA	**-1.031628**	**-1.031628**	3.54E-07
	GWO	0.999999	-0.999999	2.36E-08			GWO	**-1.031628**	**-1.031628**	2.47E-09
	PSO	**-1.0**	**-1.0**	**0**			PSO	**-1.031628**	**-1.031628**	**0**
	SCA	-0.999540	-0.998795	1.05E-02			SCA	-1.031594	-1.031584	1.43E-05

5 Conclusion

Based on the standard SSA, an adaptive attraction factor is first introduced into the follower position update formula. The follower position update thus can also be affected by the global optimal position of the population, so that the search ability and convergence speed of the algorithm is improved. Then, lens imaging and Gaussian mutation learning strategies are introduced. According to the aggregate and dispersion distribution of the current population, this strategy uses different learning strategies to mutate individuals, and enhance the population diversity and improve the escape ability of the population into local optimum. Finally, the effectiveness and superiority of the ASSA is verified by comparing the optimization results and convergence curves of seven algorithms in different dimensions of 14 benchmark functions. In the next work, the improved salps group algorithm will be considered in solving more engineering optimization problems to further verify the performance of the algorithm.

References

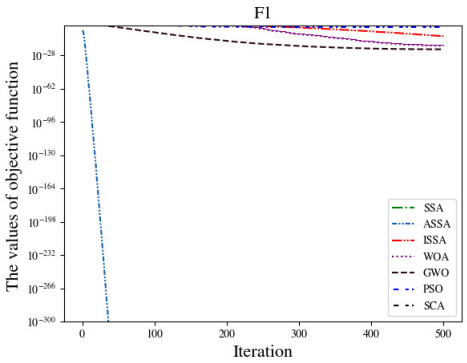
[1] S. Abd el sattar, S. Kamel, M. Ebeed, and F. Jurado, "An improved version of salp swarm algorithm for solving optimal power flow problem," *Soft Computing*, vol. 25, pp. 4027–4052, January 2021.

[2] L. Abualigah, N. K. Al-Okbi, M. A. Elaziz, and E. H. Houssein, "Boosting marine predators algorithm by salp swarm algorithm for multilevel thresholding image segmentation," *Multimedia Tools and Applications*, vol. 81, pp. 16707–16742, March 2022.

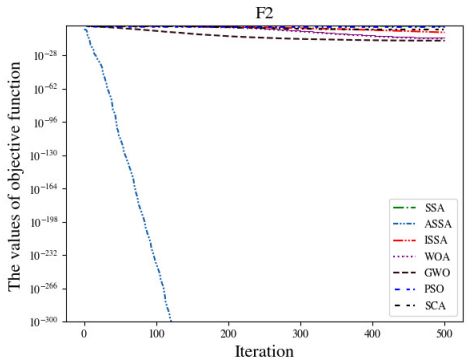
[3] Y. Bai and Z.-R. Peng, "Salp swarm algorithm based on adaptive inertia weight," *Control and Decision*, vol. 37, pp. 237–246, January 2022. (in Chinese).

[4] S. Chakraborty, A. K. Saha, S. Sharma, R. Chakraborty, and S. Debnath, "A hybrid whale optimization algorithm for global optimization," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, pp. 431–467, May 2021.

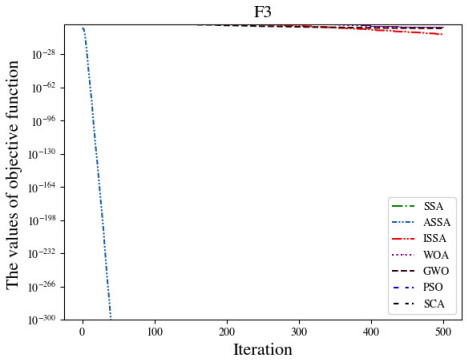
[5] M. A. Elaziz, L. Li, K. P. N. Jayasena, and S. Xiong, "Multiobjective big data optimization based on a hybrid salp swarm algorithm and differential evo-



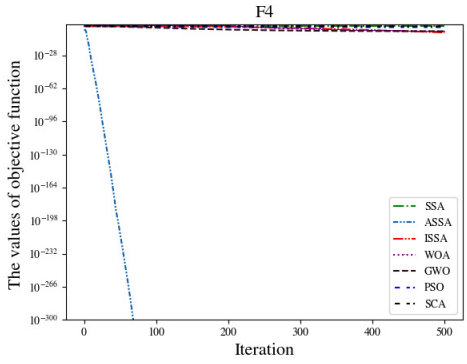
(a) $D = 50$, Convergence curve of $F_1(x)$



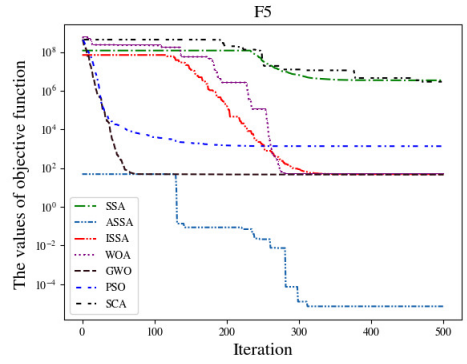
(b) $D = 50$, Convergence curve of $F_2(x)$



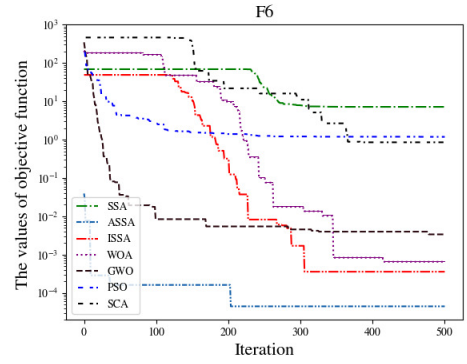
(c) $D = 50$, Convergence curve of $F_3(x)$



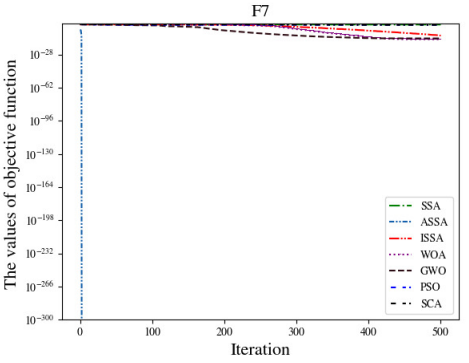
(d) $D = 50$, Convergence curve of $F_4(x)$



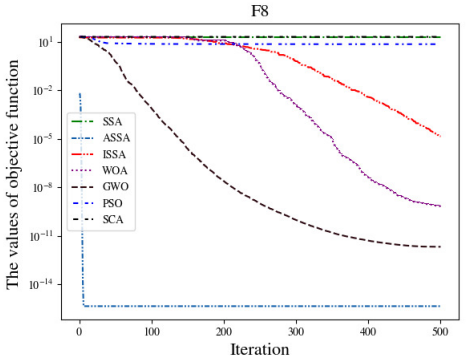
(e) $D = 50$, Convergence curve of $F_5(x)$



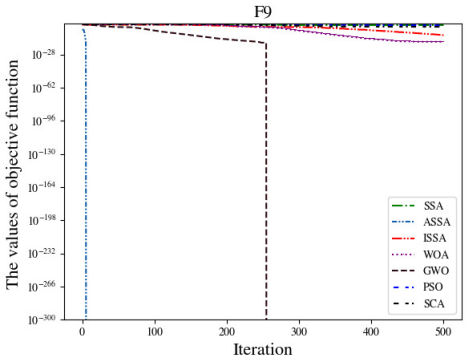
(f) $D = 50$, Convergence curve of $F_6(x)$



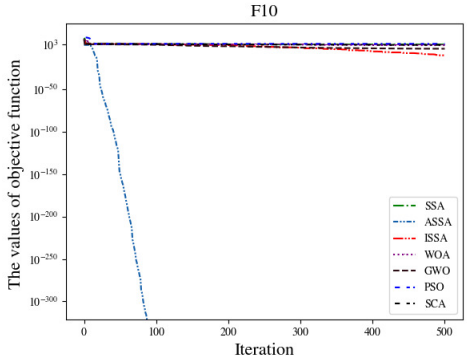
(g) $D = 50$, Convergence curve of $F_7(x)$



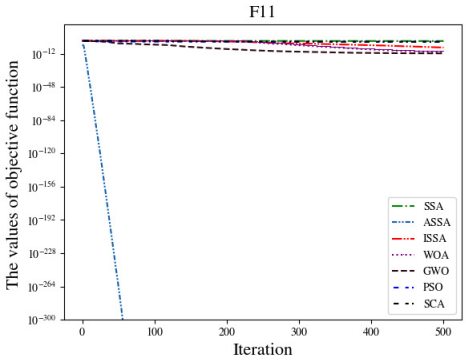
(h) $D = 50$, Convergence curve of $F_8(x)$



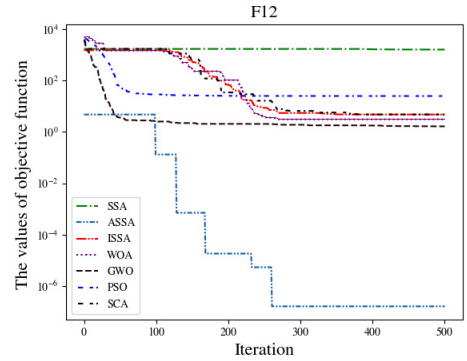
(i) $D = 50$, Convergence curve of $F_9(x)$



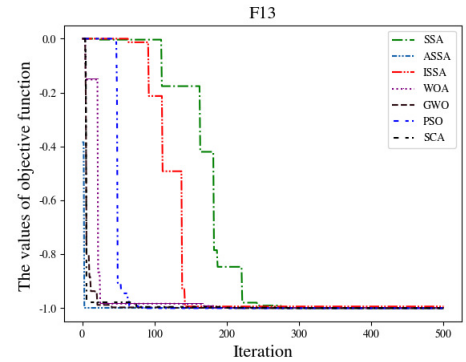
(j) $D = 50$, Convergence curve of $F_{10}(x)$



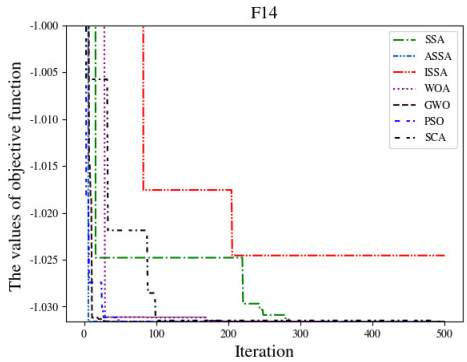
(k) $D = 50$, Convergence curve of $F_{11}(x)$



(l) $D = 50$, Convergence curve of $F_{12}(x)$



(m) $D = 50$, Convergence curve of $F_{13}(x)$



(n) $D = 50$, Convergence curve of $F_{14}(x)$

Figure 3: Comparison of the convergence curves of the seven algorithms on the benchmark functions

lution," *Applied Mathematical Modelling*, vol. 80, pp. 929–943, April 2020.

[6] Y. Fan, J. Shao, G. Sun, and X. Shao, "A modified salp swarm algorithm based on the perturbation weight for global optimization problems," *Complexity*, vol. 2020, pp. 1–17, November 2020.

[7] W. Guo, Y. He, H.-X. Chen, F.-L. Hang, and Y.-J. Li, "An abnormal login detection method based on local outlier factor and gaussian mixture model," *International Journal of Network Security*, vol. 25, pp. 297–305, March 2023.

[8] A. E. Hegazy, M. A. Makhlouf, and G. S. El-Tawel, "Improved salp swarm algorithm for feature selection," *Journal of King Saud University - Computer and Information Sciences*, vol. 32, pp. 335–344, March 2020.

[9] R. A. Ibrahim, A. A. Ewees, D. Oliva, M. A. Elaziz, and S. Lu, "Improved salp swarm algorithm based on particle swarm optimization for feature selection," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, pp. 3155–3169, September 2018.

[10] Y. Li, Y.-H. Pei, and J.-S. Liu, "Bat optimal algorithm combined uniform mutation with gaussian

mutation," *Control and Decision*, vol. 32, pp. 1775–1781, October 2017. (in Chinese).

[11] J.-S. Liu, M.-M. Yuan, and F. Zuo, "Global search-oriented adaptive leader salp swarm algorithm," *Control and Decision*, vol. 36, pp. 2152–2160, September 2021. (in Chinese).

[12] W. Long, T.-B. Wu, M.-Z. Tang, M. Xu, and S.-H. Cai, "Grey wolf optimizer algorithm based on lens imaging learning strategy," *Acta Automatica Sinica*, vol. 46, pp. 2148–2164, October 2020. (in Chinese).

[13] A.-b. Meng, Y.-c. Chen, H. Yin, and S.-z. Chen, "Crisscross optimization algorithm and its application," *Knowledge-Based Systems*, vol. 67, pp. 218–229, September 2014.

[14] S. Mirjalili, "SCA: A sine cosine algorithm for solving optimization problems," *Knowledge-Based Systems*, vol. 96, pp. 120–133, March 2016.

[15] S. Mirjalili, A. H. Gandomi, S. Z. Mirjalili, S. Saremi, H. Faris, and S. M. Mirjalili, "Salp swarm algorithm: A bio-inspired optimizer for engineering design problems," *Advances in Engineering Software*, vol. 114, pp. 163–191, December 2017.

[16] M. H. Nadimi-Shahraki, S. Taghian, S. Mirjalili, H. Zamani, and A. Bahreininejad, "GGWO: Gaze cues learning-based grey wolf optimizer and its applications for solving engineering problems," *Journal of Computational Science*, vol. 61, p. 101636, May 2022.

[17] C. Ouyang, D. Zhu, and F. Wang, "A learning sparrow search algorithm," *Computational Intelligence and Neuroscience*, vol. 2021, pp. 1–23, August 2021.

[18] N. Panda and S. K. Majhi, "Oppositional salp swarm algorithm with mutation operator for global optimization and application in training higher order neural networks," *Multimedia Tools and Applications*, vol. 80, pp. 35415–35439, January 2021.

[19] M. H. Qais, H. M. Hasanien, and S. Alghuwainem, "Enhanced salp swarm algorithm: Application to variable speed wind generators," *Engineering Applications of Artificial Intelligence*, vol. 80, pp. 82–96, April 2019.

[20] H. Ren, J. Li, H. Chen, and C. Li, "Adaptive levy-assisted salp swarm algorithm: Analysis and optimization case studies," *Mathematics and Computers in Simulation*, vol. 181, pp. 380–409, March 2021.

[21] M. A. Salam, A. T. Azar, and R. Hussien, "Swarm-based extreme learning machine models for global optimization," *Computers, Materials & Continua*, vol. 70, no. 3, pp. 6339–6363, 2022.

[22] X. Wang and J. Wang, "Research on the application of the machine learning algorithm based on parameter optimization in network security situation prediction," *International Journal of Network Security*, vol. 25, pp. 245–251, March 2023.

[23] J. Xia, H. Zhang, R. Li, Z. Wang, Z. Cai, Z. Gu, H. Chen, and Z. Pan, "Adaptive barebones salp swarm algorithm with quasi-oppositional learning for medical diagnosis systems: A comprehensive analysis," *Journal of Bionic Engineering*, vol. 19, pp. 240–256, January 2022.

[24] X.-S. Yang and A. H. Gandomi, "Bat algorithm: a novel approach for global engineering optimization," *Engineering Computations*, vol. 29, pp. 464–483, July 2012.

[25] H. Zhang, T. Liu, X. Ye, A. A. Heidari, G. Liang, H. Chen, and Z. Pan, "Differential evolution-assisted salp swarm algorithm with chaotic structure for real-world problems," *Engineering with Computers*, January 2022.

[26] Y. Zhang and X. Kong, "A particle swarm optimization algorithm with empirical balance strategy," *Chaos, Solitons & Fractals: X*, vol. 10, p. 100089, June 2023.

[27] M. Zivkovic, C. Stoean, A. Chhabra, N. Budimirovic, A. Petrovic, and N. Bacanin, "Novel improved salp swarm algorithm: An application for feature selection," *Sensors*, vol. 22, p. 1711, February 2022.

Biography

Junfu Xi, with a master's degree and an associate professor, works at Hebei University of Science and Technology and Engineering Currently, His main research interests include network security and intelligent optimization.

Yehua Chen, with a master's degree and associate professor, works in Hebei University of Science and Technology and Engineering, and studies intelligent optimization and machine learning.

Xiaoji Chen, Ph.D., associate professor, works at Hebei University of Science and Technology, majoring in software engineering and intelligent control.

Jun Li, bachelor's degree, master's degree, lecturer, professional Hebei University of Science and Technology, specially interest in field of network security.

A Defense Method Based on Moving Target Defense for New Power System APT Attack

Ruotong Li and Yuancheng Li
(Corresponding author: Yuancheng Li)

School of Control and Computer Engineering, North China Electric Power University
No. 2 Beinong Road, Changping District, Beijing, China
Email: ncepua@163.com

(Received Nov. 21, 2022; Revised and Accepted May 12, 2023; First Online June 24, 2023)

Abstract

Sensors monitoring power equipment in new power systems are vulnerable to Advanced Persistent Threat (APT) attacks, which target to tamper with transformer status signals collected by sensors. APT attackers capture one or more normal sensor nodes to obtain data from the monitoring transformer and maliciously manipulate the sensor output. Given the complexity and concealability of APT attack, Moving Target Defense (MTD) method is used to construct sensor differential immune configuration sets (M-MDCSs). Furthermore, considering the sensor cost problem, an algorithm was proposed to find the maximum value of differential immune configuration sets (M_{max}-MDCSs), and Stackelberg equilibrium was used to model the interaction between APT attacker and defender into a game form to find the sensor activation strategy. Finally, simulation experiments are carried out on the power system with standard IEEE14, 30, 118, and other nodes, and the effectiveness of the proposed method is verified.

Keywords: Advanced Persistent Threat; Moving target defense; New Power System; Stackelberg Game

1 Introduction

New power system is regarded as an important energy infrastructure in China, and its safe operation is particularly important [11]. Based on the deep integration of information technology in the traditional power system, new power system realizes the coordinated interconnection of traditional power equipments, new energy power supply and communication network [22]. However, new energy equipments in the new power system have low disturbance immunity, and system failure or extreme circumstances will affect the safety of the power system [23].

At present, the power system deploys sensors in substations and transmission lines, which can analyze sensor data to monitor the running status of power equipments in real time [13]. Given the time-sensitivity and criticality of sensor measurements, sensors have become attractive targets for malicious attackers [15]. Attackers physically attack the power system by manipulating the sensor measurements transmitted from the on-site power equipment to the control center [10]. The malicious activity of the attacker against the measured value of the sensor may affect the normal control operation of the operator in the control center, thus further causing economic losses and equipment damage [9].

Among the many attacks forms against sensors, Advanced Persistent Threat (APT) attack is one of the most threatening attacks. The malicious activities of APT attackers are usually realized by operating sensor signals and transmitting error information to the control center, thus affecting the state estimation results of the power system and threatening the safe operation of the power system [5].Sensor is an important measuring device for monitoring power equipment, and its data error will lead to serious consequences. For example, in 2015, the Ukrainian power grid was attacked by BlackEnergy. The attacker sent spam containing malicious files to gain control rights of the power system and manipulate the circuit breaker. In addition, in order to prevent system recovery after power failure, the attacker destroys the data storage system through malicious components in advance, erases the intrusion traces, and then attacks the control center to prevent the control center from obtaining power failure messages in advance [8].

In 2019, more than 70% of Venezuela's regions had power outages, most of which had power outages for more than one day. The attacker launched an attack by implanting malicious software into some important components, resulting in the shutdown of the largest Guri hydropower station unit in Venezuela, and implemented interference behavior on the hydropower station unit in the subsequent recovery process [19]. Therefore, it is urgent to study the APT attack defense methods against sensors in the new power system to ensure the normal operation of the new power system.

2 Related Work

In recent years, some scholars at home and abroad have conducted relevant research on the defense of APT attacks of sensors. Literature [12] built a game model for both sides of attack and defense in view of the sensor being attacked by malicious programs. Through the analysis of the evolution process of the strategies of both attack and defense sides, we get the strategies to inhibit the spread of malicious programs between sensors. However, due to the volatility of game returns and other factors, the evolutionary game model can no longer fully simulate the impact of the model under multi factor changes. Literature [7] proposed a zero-sum game method to defend against malicious attacks, but due to the computational amount of the algorithm, it is not applicable to large power systems. Literature [20]studied the overall network physical solutions to APT attacks, which considered the coupling between the two layers of the system, and proposed a collaborative design defense mechanism against APT attacks. Literature [16]considered the problem of hiding the activation of moving target defense from the attacker and proposed the so-called invisible moving target defense, but it did not consider the use of moving target defense method to solve the problem of APT attack information system resulting in the failure of the physical system.

Therefore, aiming at the problem of APT attack sensor in new power system, this paper creatively proposes a defense method based on moving target defense [3,21]. APT attackers select sensor nodes to attack according to different attack costs, and then maliciously manipulate sensor measurement data output by attacking one or more normal sensor nodes. Therefore, it is necessary to consider sensor deployment to defend against APT attacks. Firstly, sensor differential immune configuration sets (M-MDCSs) are constructed based on the moving target defense method. M-MDCSs constrain that any two configuration sets are not allowed to share the same sensor, and different configuration sets are allowed to uniquely identify specific transformers, which considers the robustness of sensor deployment mechanism in response to APT attacks. Considering the sensor cost problem, an algorithm for finding the maximum value of differential immune configuration set (M_{max}-MDCSs) is proposed. Finally, the interaction between attacker and defender is modeled as Stackelberg game to find sensor activation strategy. Experimental results show that in IEEE14 bus, IEEE30 bus and IEEE118 bus system, the proposed method has better defense effect compared with the method of using greedy algorithm to deploy sensors to defend APT attacks.

3 Problem Description

While providing operation control support for the new power system, the application of information technology in the physical system of the power system also greatly improves the risk of physical equipment being attacked [17], and the risk of APT attack also greatly increases.Different from the attack behavior that only stays at the information level, APT attack is a long-term and persistent attack behavior with latent and secret characteristics. In recent years, APT attack has shown strong cross-platform characteristics [6], gradually penetrating into the physical process of the power system, making the traditional passive defense system ineffective.The architecture of new power system is shown in Figure 1. APT attack of new power system against sensors mainly occurs in the position shown in Figure 1. When the transformer in the power domain generates fault signals, the sensor collects signals and prepares to transmit the fault signals to the information domain. At this time, the attacker with reconnaissance capability captures the sensor node to obtain signal data and maliciously manipulates the sensor to output data to the information domain, thus threatening the normal operation of new power system.Therefore, it is of great significance to study moving target defense method against APT attacks of sensors.

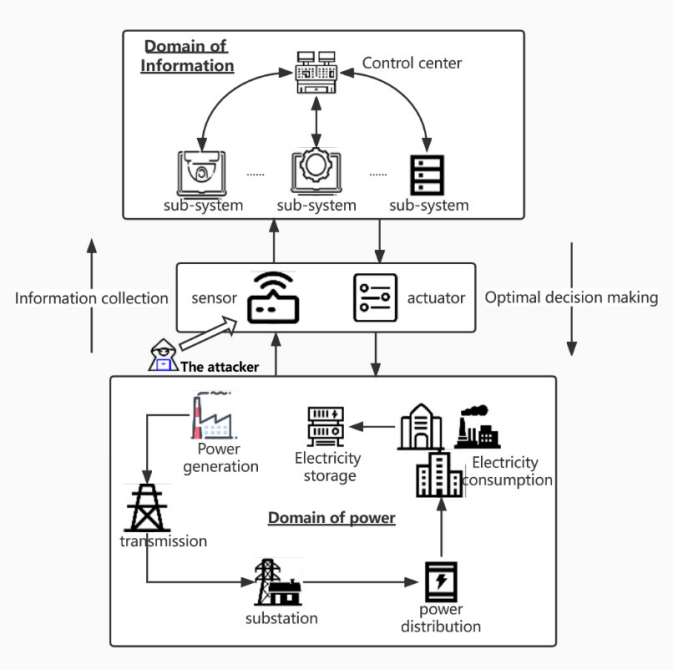


Figure 1: Architecture of new power system

4 A Defense Method Based on Moving Target Defense for New Power System APT Attack

Moving Target Defense [18] (MTD) seeks to constantly move between a set of system configurations available to the defender, so that the attacker will not encounter the expected system configuration when attacking, thus rendering the attack ineffective in order to take away the attacker's reconnaissance advantage. We use triples (C, T,

M) to describe MTD, where C represents sensor configuration sets of the defender's response to the attack strategy, T represents the time function describing the defender's movement, and M represents the movement strategy.The ultimate goal of the defense against APT attacks in this paper is to dynamically activate the constructed differential immune configuration sets to avoid APT attack, so as to ensure the normal transmission of signals from sensors to the information domain and achieve the defense effect. The specific flow of defense against APT attack sensor of new power system based on moving target defense is as follows:

1) The monitoring process of the sensor on the transformer in the power system is modeled into a bipartite graph, and the differential immune configuration sets are constructed by considering the location of the sensor;

2) The linear programming method is used to add constraints to the differential immune configuration sets to find the maximum value of the sensor differential immune configuration set for monitoring a specific transformer;

3) The interaction between the attacker and the defender is modeled as Stackelberg game. The defender deploys sensors according to the differential immune configuration sets. The attacker realizes the defender's defense strategy at the current stage and gives the optimal attack strategy at the stage, while the defender chooses the optimal activation strategy for APT attack.

4.1 Differential Immune Configuration Sets (M-MDCSs)

The minimum discriminant code set [4] (MDCS)is a special case of the minimum identification code set [14] (MICS). For a bipartite diagram of the power system, MDCS is the minimum set of nodes where sensors can be deployed under certain constraints. The IEEE14 bus of the power system is used as an example to describe MDCS. Firstly, a bipartite graph $G = (T \cup S, E)$ is built, where T represents the set of transformers that need to be monitored exclusively, S represents the position where the sensor can be deployed, and E represents the edge set that exists when the operation behavior signal of the transformer reaches the sensor within the hop number of 2 (the hop number represents the distance that the signal of the transformer can be received in the bipartite diagram. According to literature [2], the hop number is 2). We define MDCS as follows: If $\forall$ t $\in T$, N(t) $\cap$ $S_0 \subseteq S$ is unique, then define that node set S_0 is the MDCS of G, where N(t) represents the neighborhood of t.The constructed bipartite graph G is shown in Figure 2. Yellow nodes represent buses, red squares represent transformers, green squares represent locations where sensors can

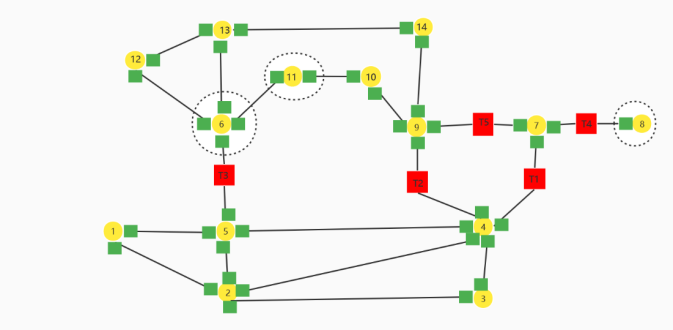


Figure 2: Bipartite Graph G

be deployed, and Dashed circles represent MDCS, each of which uniquely identifies the 5 transformers in the graph.

In order to prevent a single attack from destroying all sensor deployments, we propose the definition of differential immune configuration sets: given a bipartite graph $G = (T \cup S, E)$, M vertex sets $S_i \subseteq S$ (i $\in \{1, ..., M\}$)) are defined as the M-MDCSs of G, where all sets S_i are MDCS and for all possible set pairs (S_i,S_j)(i$\neq$ j), $S_i \cap S_j = \emptyset$,that is, any two MDCS are not allowed to share a node where sensors are deployed. This definition ensures that when APT attacker attacks a specific node s $\in$ S where sensors are deployed, the attacker can only weaken at most one MDCS ($S_i \in$ C) so that it cannot uniquely identify transformer state signals. At this time, the defender chooses to activate other MDCS ($S_j \in$ C) to identify and obtain the transformer status signal, and the attacker will not be able to affect the normal realization of sensor functions.

Defenders need to deploy M*m sensors in the power system and activate MDCS (the size of MDCS is m) at any point in time to uniquely identify the transformer's status signal. While deploying a large number of MDCS helps to increase the options for activating sensors, thereby reducing the success rate of APT attacker, it also incurs M*m sensor costs. Therefore, on the basis of considering the cost, we propose an improved linear programming (Q-ILP) method to solve the differential immune configuration set in the case of minimum value n, where n represents the size of each Discriminating Code Set (DCS). Q-ILP method is described as follows:

$$\min_{n,x} n \tag{1}$$

$$s.t.\ n = \sum_{s} x_{sm} \quad \forall m \tag{2}$$

$$\sum_{s \in S} (x_{sm} - x_{sm`})^2 = 2n \quad \forall (m, m`) \tag{3}$$

$$x_{sm} \in \{0, 1\} \quad \forall s, \forall m \tag{4}$$

The objective function is expressed as (1) to solve the differential immune configuration set constructed with the least number of sensors. For the m-th DCS (m $\in \{1, ..., |S|\}$), $x_{sm} = 1$ if sensor is placed in node s $\in$ S, otherwise 0. Constraints (2) and (3) ensure that each

DCS is equal in size and that no two DCS share the same sensor. We also need to ensure that all DCS obtained are discriminant code sets, so add Constraints (5) and (6) on the basis of the above three constraints:

$$\sum_{s\in N(t)} x_{sm} \geq 1 \quad \forall t, \forall m \tag{5}$$

$$\sum_{s\in N(t)\triangle N(t^{'})} x_{sm} \geq 1 \quad \forall (t,t^{'}), \forall m \tag{6}$$

Where N(t) represents the neighborhood of t, and $N(t^{'})$ represents the neighborhood of $t^{'}$. Constraint (5) ensures that t ∈ T triggers at least one sensor s, Constraint (6) ensures that for all $(t,t^{'})(t^{'} \in \mathrm{T})$, there is at least one sensor in the symmetric difference set of t and $t^{'}$ that is part of the DCS and uniquely recognizes t and $t^{'}$.

4.2 Find the maximum value of differential immune configuration sets (M_{max}-MDCSs)

When the defender has enough defense resources, for bipartite graph $G = (T \cup S, E)$, t ∈ T,N(t) = {s},s ∈ S,any MDCS of G would require a sensor to be deployed on s to uniquely monitor the fault signal in t. Therefore, there cannot be two MDCS that do not share a common node, because s must be part of both MDCS. In this case, the maximum value of M (denoted as M_{max}) is 1. However, considering the cost in reality, we cannot deploy sensors on all s, so we need to conduct a search process on the search space of m we described to find the maximum differential immune configuration sets (M_{max}-MDCSs).Therefore, we proposed an optimal algorithm to solve M_{max}-MDCSs, and the algorithm flow is shown in Figure 3. Firstly, the Q-ILP method is used to solve M-MDCSs successively in the search space of m, and the results of each solution are compared with the results of the last solution. If the length of each DCS in the solved M-MDCSs is minimum or all solutions in the search space are completed, the solution process is finished. The resulting M-MDCSs is M_{max}-MDCSs.Otherwise, the loop continues to solve M_{max}-MDCSs.

Figure 4 shows the M_{max}-MDCSs solution returned by the optimal algorithm in Figure 2, where M_{max} is 4. Each line of color combination represents a different MDCS, and each line of color combination below T_i (i ∈ {1, ..., 5}) represents DCS. As shown in the figure, each of the four MDCS has a size of n = 3 and uniquely monitors all transformers T_i.The absence of overlapping colors in the bottom node set indicates that no two MDCS share the same s ∈ S.

4.3 Optimal differential immune configuration sets activation strategy

The goal of the defender is to ensure that the transformer status signal is only monitored under any circumstances, while the goal of the attacker is to make it more difficult

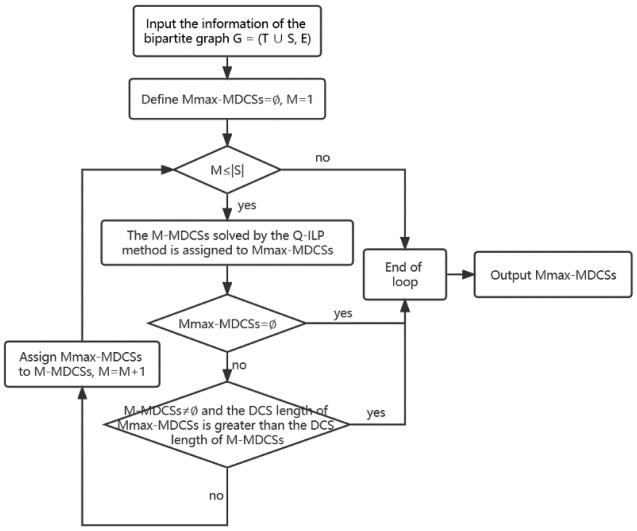


Figure 3: Flow chart of solving M_{max}-MDCSs optimal algorithm

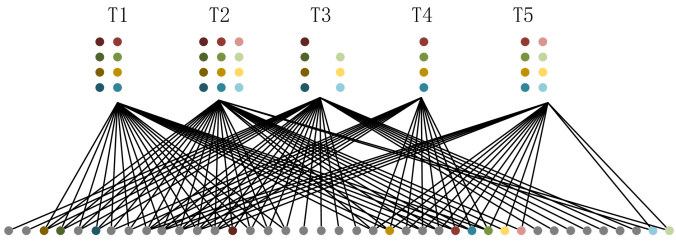


Figure 4: 4-MDCSs returned by the optimal algorithm

for the defender to effectively monitor the transformer status signal. Therefore, we consider a threat model in which an attacker with reconnaissance capability is aware of the sensor activation strategy of the defender, and we use Stackelberg equilibrium to solve the activation strategy of the defender's optimal differential immune configuration sets [1]. We seek to use MTD to activate the sensor's optimal movement function M to help the defenders achieve the goal. We briefly describe the various parameters of this game strategy, as shown in Figure 5.

In Figure 5, the first row represents the sensor node attacked by the attacker, and the first column represents the sensor activation strategy of the defender. In the lower right corner of the diagram, since the attacker attacks the sensor represented by the light blue node, the defender can only uniquely identify the transformer T_3 and therefore only receive a reward proportional to it. On the contrary, by attacking a sensor, the attacker can make the fault signals of transformers T_1 and T_2 (as well as T_4 and T_5) indistinguishable and obtain the corresponding reward P^D.Then the reward obtained by the attacker is expressed as P^D minus the cost of attacking the sensor represented by the light blue node. Similarly, if the at-

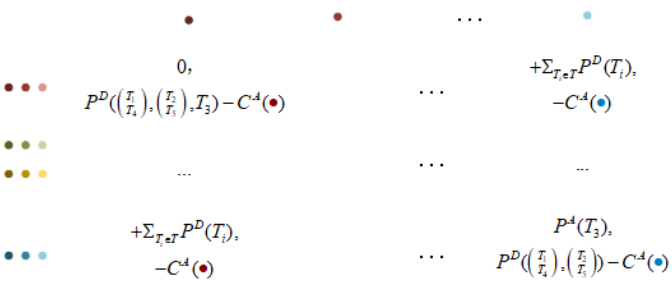


Figure 5: Revenue matrix of both sides in game

tacker chooses to attack the sensor represented by dark brown nodes, the defender will not be able to identify any transformer, so the reward for the defender is zero.The attacker can make the fault signals of transformers T_1 and T_2 (as well as T_4 and T_5) indistinguishable and obtain the corresponding reward P^D. Then, the reward obtained by the attacker is expressed as the reward P^D obtained when the fault signals of transformers T_1 and T_2 (as well as T_4 and T_5) are indistinguishable, minus the cost of attacking the sensor represented by the light blue node.

The defender has the M_{max} pure strategy, and configuration set C = M_{max}-MDCS.The sets of action of the attacker include attack a sensor may be considered activation (not all the nodes in the $|S|$). Our description of solving the optimal movement function M of the sensor activated by MTD is as follows:

$$max(\sum_{l\in L, i\in X, j\in Q} P_l * R_{lij} * Z_{lij})$$

$$s.t. \sum_{i\in X}\sum_{j\in Q} Z_{lij} = 1$$

$$\sum_{j\in Q} Z_{lij} \leq 1$$

$$q_{lj} \leq \sum_{i\in X} Z_{lij} \leq 1$$

$$\sum_{j\in Q} q_{ij} = 1$$

$$0 \leq a_l - C_{lij} * \sum_{j\in Q} Z_{lij} \leq (1-q_{lj}) * M$$

$$0 \leq Z_{lij} \leq 1, \forall l \in L, \forall i \in X$$

Where L represents the attacker set, l represents an attacker, X represents the defense policy set of the defender, Q represents the attack policy set of the attacker, P_l represents the probability of the differential immune configuration set of the attack sensor of the attacker, R_{lij} represents the reward of the defender when the L-th attacker uses attack strategy j and the defender uses defense strategy i.Z_{lij} j represents the probability of the defender using defense policy i when the L-th attacker uses attack policy j,q_{lj} represents the attack policy j of the L-th attacker, a_l represents the maximum reward for the L-th attacker, C_{lij} represents the reward for the L-th attacker when the L-th attacker uses attack policy j and the defender uses defense policy i, and M represents the maximum value.

5 Experiment and analysis

In order to verify the effectiveness of the defense method based on moving target defense for new power system APT Attack, we have carried out experimental research on IEEE14 bus, IEEE30 bus and IEEE118 bus system, and compared the optimal algorithm with the common greedy algorithm when solving M_{max}-MDCS, and Stackelberg game strategy was compared with the uniform random strategy (selecting an equal probability to activate a MDCS). Finally, it is proved that the proposed method has better defense effect against APT attacks of new power systems.

5.1 Experimental preparation and experimental environment

The server version used in this paper is Ubuntu 16.04, NVIDIA TITAN RTX 2080Ti graphics card and CUDA 11.2. The experimental environment was python 3.7, and the optimal algorithm is written using the tensorflow framework. In the training process of the model, Gurobi solver is used to optimize the model parameters. In the Gurobi solver, in order to obtain high-quality feasible solutions faster, the whole algorithm takes mathematical programming as the framework, and at the same time, heuristic algorithms are used in individual links.

5.2 Evaluation method

In order to accurately evaluate the effectiveness of Q-ILP method and optimal algorithm against APT attacks proposed in this paper, we verify the effectiveness from the following two performance indicators:

1) Defense gains:

$$Price = \sum_{l\in L, i\in X, j\in Q} P_l * R_{lij} * Z_{lij} \quad (7)$$

In Formula (7), L represents the set of attackers, l represents an attacker, X represents the defender's defense strategy, Q represents the set of attackers' attack strategies, and P_l is the probability of attacker's attack sensor differential immune configuration set, R_{lij} represents the defender's reward when the first attacker uses attack strategy j and the defender uses defense strategy i, Z_{lij} indicates the probability that the defender uses defense strategy i when the first attacker uses attack strategy j.

2) The time spent by greedy algorithm and optimal algorithm and the number of sensors deployed on each node bus.

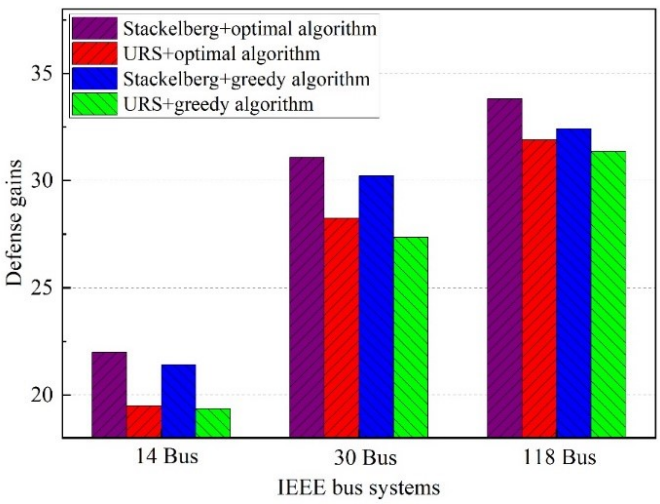


Figure 6: Defense benefits of different node bus systems

5.3 Experimental comparison

In this section,We have carried out experimental research on IEEE14 bus, IEEE30 bus and IEEE118 bus systems in the popular IEEE test charts in the power field [24].We compare the optimal algorithm and greedy algorithm proposed in this paper under the Stackelberg Equilibrium Strategy and Uniform Random Strategy (URS) respectively. The experimental results are shown in Figure 6.

It can be seen from the figure that in the case of IEEE14 bus, IEEE30 bus and IEEE118 bus systems, no matter which algorithm is selected to solve the optimal differential immune configuration set, the optimal mobility strategy of Stackelberg is more beneficial to the defender than URS. Specifically, when the optimal algorithm is selected to solve the optimal differential immune configuration set in the IEEE14 bus, IEEE30 bus and IEEE118 bus systems, the optimal moving strategy benefit of Stackelberg is 2.5, 2.75 and 2.29 higher than that of URS. In the IEEE14 bus, IEEE30 bus and IEEE118 bus systems, whether URS or Stackelberg is selected, the defense benefit of the optimal algorithm to solve the optimal differential immune configuration set is always higher than that of the greedy algorithm.

When sensors in new power system are attacked by APT, the longer the APT attack exists in new power system, the greater the impact on the normal operation of new power system. Therefore, the shorter the time required to find and activate differential immune configuration sets, the better. We carried out a comparative experiment on the time of searching and activating the differential immune configuration sets by the optimal algorithm and greedy algorithm of different node bus systems, the experimental results are shown in Table 1. Where N represents the total number of nodes (the sum of transformer nodes and deployable sensor nodes of different node bus systems), A^D (M_{max} / M) represents the defense strategy, and A^A (M_{max} / M) represents the attack strategy. It can be seen from Table 1 that although the number of differential immune configuration sets solved by optimal algorithm and greedy algorithm is the same in IEEE14 bus, IEEE30 bus and IEEE118 bus systems, the time spent by optimal algorithm to find differential immune configuration sets is significantly shortened.

We also consider this situation. When the defender determines the differential immune configuration set in advance to limit the placement cost of sensors in the power system, the greedy algorithm needs to find a solution iteratively and add them to the constraint set of the next iteration until the required differential immune configuration set is found. In this case, we can completely ignore the iterative process in the optimal algorithm proposed in this paper and directly return the solutions found in Formulas (1) to (5).

6 Conclusions

Aiming at the problem of APT attack sensors in new power system, this paper proposes a defense method based on moving target defense for new power system APT attack. Firstly, the monitoring process of sensors to transformers in power system is modeled as a bipartite graph, and the location of deployable sensors is considered to construct a differential immune configuration sets (M-MDCSs). Secondly, a Q-ILP method is proposed to add constraints to the differential immune configuration sets to find the optimal differential immune configuration sets; Finally, the interaction between attackers and defenders is modeled as the Stackelberg game to find the optimal activation strategy of differential immune configuration sets. In addition, this paper has carried out simulation experiments on IEEE14 bus, IEEE30 bus and IEEE118 bus systems, and obtained the following conclusions:

1) A Q-ILP method is proposed to solve the differential immune configuration sets (M-MDCSs), which ensures that multiple sensors have only one monitoring transformer to resist APT attack and ensure the sensor's fault tolerance.

2) An optimal algorithm is proposed to find the optimal activation strategy of the differential immune configuration sets. Compared with the greedy algorithm, the optimal algorithm takes less time to find the differential immune configuration sets when the number of differential immune configuration sets is the same.

3) The interaction between the attacker and the defender is modeled as the Stackelberg game. No matter which algorithm is selected to solve the optimal differential immune configuration sets, the optimal mobility strategy of Stackelberg will obtain higher defense benefits than the optimal mobility strategy of URS.

Table 1: **Time spent by different node bus systems to find differential immune configuration set**

Differential immune configuration set C				Time spent looking for C (unit/s)	
Bus system	N	$A^D(M_{max}/M)$	$A^A(M_{max}/M)$	Optimal algorithm	greedy algorithm
IEEE14	45	4/4	12/12	0.019	0.083
IEEE30	89	4/4	16/16	0.038	0.20
IEEE118	367	2/2	10/10	0.56	45.92

Acknowledgments

This work was supported by the State Grid Corporation Science and Technology Project "Research on the Identification and Active Defense of Advanced Persistent Threat for New Power System" under Grant 5700-202199539A-0-5-ZN.

References

[1] S. M. Ananthanarayanan, C. Kroer, "Computing the optimal distributionally-robust strategy to commit to," *arXiv:2209.07647v1*, 2022.

[2] K. Basu, M. Padhee, S. Roy, A. Pal, A. Sen, M. Rhodes, B. Keel, "Health monitoring of critical power system equipments using identifying codes," in *CRITIS*, Lecture Notes in Computer Science, vol. 11260, pp. 29–41, 2018.

[3] M. Cui, J. Wang, "Deeply hidden moving-target-defense for cybersecure unbalanced distribution systems considering voltage stability," *IEEE Transactions on Power Systems*, vol. 36, no. 3, pp. 1961–1972, 2021.

[4] S. Dey, F. Foucaud, S. C. Nandy, and A. Sen, "Discriminating codes in geometric setups," 2020. (`https://drops.dagstuhl.de/opus/volltexte/2020/13368/pdf/LIPIcs-ISAAC-2020-24.pdf`)

[5] W. M. He, S. Li, C. K. Ahn, J. Guo, and Z. R. Xiang, "Sampled-data stabilization of stochastic interconnected cyber-physical systems under dos attacks," *IEEE Systems Journal*, vol. 16, no. 3, pp. 3844–3854, 2022.

[6] J. Hou, L. Sun, T. Shu, and H. Li, "The value of traded target information in security games," *IEEE/ACM Transactions on Networking*, vol. 29, no. 4, pp. 1853-1866, 2021.

[7] R. James, B. Sikdar, "Detection of stealthy cyber-physical line disconnection attacks in smart grid," *IEEE transactions on smart grid*, vol. 12, no. 5, 2021.

[8] T. T. Ji, B. X. Fang, X. Cui, Z. R. Wang, R. L. Gan, Y. Han, and W. Q. Yu, "Research on deep learning-powered malware attack and defense techniques," *Chinese Journal of Computers*, vol. 44, no. 4, pp. 669–695, 2021.

[9] M. N. Kurt, Y. Yılmaz, and X. Wang, "Distributed quickest detection of cyber-attacks in smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2015–2030, 2018.

[10] S. Lakshminarayana, E. V. Belmega, and H. V. Poor, "Moving-target defense against cyber-physical attacks in power grids via game theory," *IEEE Transactions on Smart Grid*, vol. 12, no. 6, pp. 5244–5257, 2021.

[11] X. Li, J. B. Xu, M. L. Li, M. Ni, and H. Q. Tong, "A security evaluation method for cyber physical distribution system considering influence of information failure," *Electric Power*, vol. 55, no. 2, pp. 73–81, 2022.

[12] P. Maheshwari, A. K. Sharma, K. Verma, "Game theoretic application for energy efficient mobility handling in wireless sensor network," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 9, 2020.

[13] G. C. Montanari, R. Hebner, P. Seri, and R. Ghosh, "Self-assessment of health conditions of electrical assets and grid components: A contribution to smart grids," *IEEE Transactions on Smart Grid*, vol. 12, no. 2, pp. 1206–1214, 2021.

[14] R. Nikandish, O. K. Nasab, E. Dodonge, "Minimum identifying codes in some graphs differing by matchings," *Discrete Mathematics, Algorithms and Applications*, vol. 12, no. 3, 2020.

[15] S. Pal, B. Sikdar, and J.H. Chow, "An online mechanism for detection of gray-hole attacks on pmu data," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2498–2507, 2018.

[16] J. Tian, R. Tan, X. Guan, T. Liu, "Enhanced hidden moving target defense in smart grids," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2208–2223, 2019.

[17] J. S. Wang, G. H. Yang, "Data-driven methods for stealthy attacks on tcp/ip-based networked control systems equipped with attack detectors," *IEEE Transactions on Cybernetics*, vol. PP, pp. 1–12, 2019.

[18] Y. Wang, X. Xiong, C. Gao, "Mtdcd: A hybrid defense mechanism against network intrusion," *Computer Science*, vol. 49, no. 7, 2022.

[19] Z. J. Wang, Y. Liu, Y. Y. Bao, X. H. Guan, T. Wu, J. G. Lu, Z. W. Yu, X. S. Yuan, and J. Liu, "Power system security simulation technologies: engineering safety, network security and cyber-physical integrated security," *SCIENTIA SINICA Informationis*, vol. 52, no. 3, pp. 399–429, 2022.

[20] C. Wu, W. Yao, W. Pan, G. Sun, and L. Wu, "Secure control for cyber-physical systems under malicious attacks," *IEEE Transactions on Control of Network Systems*, vol. PP, no. 99, pp. 1–1, 2021.

[21] H. Zhang, J. Wang, L. Jiang, "A markov signaling game - theoretic approach to moving target defense strategy selection," *Acta Electronica Sinica*, vol. 49, no. 3, pp. 527–535, 2021.

[22] Z. G. Zhang and C. Q. Kang, "Challenges and prospects for constructing the new-type power system towards a carbon neutrality future," *Proceedings of the CSEE*, vol. 42, no. 8, pp. 2806–2819, 2022.

[23] Y. Zhao, S. Xia, J. Zhang, M. Wu, "Effect of the digital transformation of power system on renewable energy utilization in China," *IEEE Access*, 2021.

[24] R. D. Zimmerman, C. E. Murillo-Sánchez, R. J. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, 2011.

Biography

Ruo-tong Li biography. She was born in Jan. 1999. She is a master student at North China Electric Power University. Her major research field is power system information security. E-mail: CY2110054@163.com.

Yuan-cheng Li biography. He was born in Aug. 1970. He is a professor and a supervisor of Doctoral student at North China Electric Power University. His major research field is information security and privacy protection, cryptography and blockchain, artificial intelligence and security. E-mail : ncepua@163.com.

A More Secure and Revocable Anonymous Authentication Scheme for IoT

Mana Mao[1], Jiujiu Yu[2], and Yimin Wang[1]
(Corresponding author: Yimin Wang)
The School of Information and Computer, Anhui Agricultural University, Anhui, China[1]
Email: ymw@ahau.edu.cn
The School of Computer Engineering, Anhui Sanlian University, Anhui, China[2]
(Received Nov. 24, 2022; Revised and Accepted May 12, 2023; First Online June 24, 2023)

Abstract

The Internet of Things (IoT) application has become ever more common these days and ensures greater convenience in industrial production, medical treatment, and daily life. However, while users are authorized to access and control devices remotely, insecurity of data transmission and user privacy issues are still present. Numerous researchers have suggested various anonymous authentication schemes. Patel *et al.* proposed an efficient and dependable lightweight Remote User Authentication scheme (RUA). Nevertheless, it was discovered that this scheme does not achieve anonymity or un-linkability. We propose a secure and efficient two-factor authentication and key agreement scheme based on Elliptic Curve Cryptography (ECC), which retains the advantages of the Patel *et al.* scheme while also providing user anonymity and a revocation mechanism. Each time the user logs in to access the device, the user and the gateway will form a new session key after mutual authentication, which ensures the user's anonymity and incontestability. Compared with the schemes of Patel *et al.*, this scheme is much more secure and more appropriate for the IoT at the equivalent cost.

Keywords: Anonymous Authentication; ECC; IoT; Revocation

1 Introduction

With the development of Internet technology, the IoT, as the symbol of a new generation of industrial revolution technology, closely links enterprises, devices, individuals and families [13, 15]. With the IoT, users can realise information exchange between things and things, things and people through a range of information sensing devices such as global positioning systems, radio frequency identification technology, infrared sensors and so on [4, 8, 17]. The structure of a typical IoT is shown in Figure 1, there are three main entities in IoT: The first layer is the perception layer, which is composed of various sensor nodes and is responsible for information collection and transmission [1]. The second layer is the network layer, which is composed of gateway, cloud authentication server and data storage server. Wireless and wired networks are used to encode, authenticate and transmit the data gathered. The rapid development of WiFi, 4G, 5G and other network technologies provides a good network environment for the development of the IoT [14]. The third layer is the application layer, which is composed of various user terminal devices and is applied to green agriculture, telemedicine, intelligent transportation, smart home, urban management, etc. The user can monitor the working state of the equipment and control the equipment at any time and location [2, 10].

Even though the IoT has brought great convenience to human production and life, due to the insecurity of its information transmission channels, unauthorised users can illegally gather sensor data, so the data privacy and personal security of IoT still face numerous problems [18]. Therefore, more and more researchers are paying attention to and studying conditional privacy-preserving authentication schemes. Patel *et al.* [10] proposed an efficient and reliable lightweight remote user authentication scheme with mutually verified secret key exchange for the user gateway model. They used Dolev-Yao channel to informally analyze the proposed scheme and BAN logic to provide mutual authentication verification for the scheme. Nevertheless, this it does not appear to achieve anonymity and un-linkability. Based on Patel *et al.*'s [10] RSU scheme, we suggest a more secure and revocation anonymous authentication scheme. This contribution chiefly includes the following points:

- Through careful analysis of RUA scheme [10], it can not achieve anonymity and un-linkability, and there is no revocation mechanism.
- A new scheme is proposed in this paper. When the user login needs the gateway to verify his identity, the user ID is encrypted by the random number generated by the user's device and the system public key to

generate a pseudonym, which realizes the anonymity and un-linkability of the scheme.

- The scheme also adds an efficient revocation mechanism. When a malicious user appears, simply add it to the Certificate Revocation List (CRL) to remove it.

The composition of the paper is as follows. In Section 2, we briefly present related work on IoT security authentication. In Section 3, the system model and security requirements based on the scheme are introduced in detail. In Section 4, we review the RUA scheme and present its security analysis. In Section 5, we present the proposed scheme in detail. In Section 6, We analyze the security and evaluate the performance of our scheme. Finally, we conclude the scheme in Section 7.

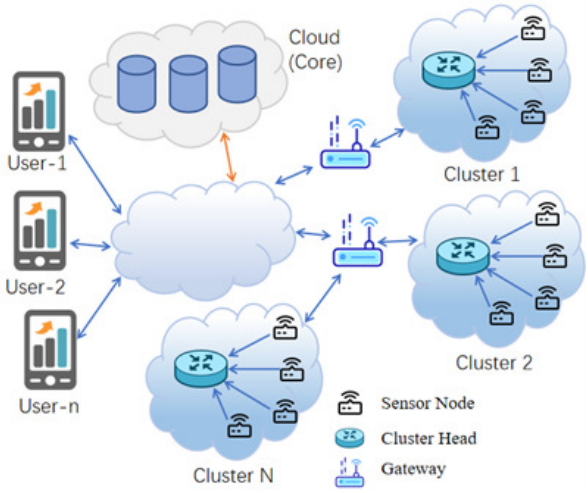


Figure 1: Typical IoT structurel

2 Related Work

In current years, with the frequent occurrence of IoT security incidents, great security risks have been brought to industrial production and people's daily lives. Faced with the many security and privacy issues in IoT numerous researchers have proposed various solutions, which generally include the use of diverse factors such as password, biometric and smart card (SC) to authenticate authorised users [4, 7].

In 2004, Das, Saxena and Gulati [3] proposed a dynamic ID-based remote user authentication scheme using SC. Their scheme allows users to change and choose passwords freely, and the server does not maintain any verifier table. However, researchers have been done to point that it is completely insecure for its independent of the password. Furthermore, it did not achieve mutual authentication and could not resist impersonate remote server attack. In 2009, Wang *et al.* [16] offered an enhanced password authentication scheme and reviewed Das *et al.*'s [3] scheme which keeps the merits of the original scheme. However, Khan *et al.* [6] showed that Wang *et al.*'s [16] scheme cannot revoke the lost or stolen SC, does not support the establishment of session secret key between the user and the server, and the user's password is assigned by the server cannot choose by himself. Therefore, Khan *et al.* [6] proposed an enhanced SC-based identity authentication scheme, which improves all the drawbacks of Wang *et al.*'s [16] scheme. In 2014, Xu *et al.* [19] designed a protocol for two-factor mutual authentication with key agreement protocol using ECC for TMIS service. This scheme cannot resist replay attack and users cannot update passwords. Islam *et al.* [5] improved the problem of Xu *et al.*'s [19] scheme, and they claimed that their protocol is not only efficient, but also satisfies all security requirements. However, Chaudhry *et al.* [12] pointed out that Islam *et al.*'s [5] protocol suffers from user impersonation and server impersonation attacks. Chaudhry *et al.* [12] proposed an identity authentication scheme based on ECC and temporary ID and claimed that their scheme can resist privileged insider attack, impersonation attack and replay attack. In 2017, Qiu *et al.* [11] proved that the scheme proposed by Chaudhry *et al.* [12] could not resist password guessing attack and user impersonation attack and proposed an improved authentication scheme. In 2020, Patel *et al.* [10] proved that Qiu *et al.*'s [11] scheme did not have perfect forward secrecy and could not resist gateway impersonation attack and denial of service attack. Therefore, Patel *et al.* [10] proposed a lightweight RUA scheme based on ECC. An identity-based conditional privacy protection scheme based on Patel *et al.* [10] and Odelu *et al.*'s scheme [9] is proposed. The comparison of some schemes with the proposed scheme are listed in Table 1.

3 Preliminarties

This section presents the two parts needed to build the scheme: the system model and the security requirements.

3.1 System Model

As shown in Figure 1, a complete IoT consists of a gateway node, a set of users and a set of sensors. The main functions of each entity in IoT system are described as below.

GATEWAY. This authoritative entity is universally trusted and placed in a secure environment. When a new user joins the IoT, the gateway needs to verify the legitimacy of the user's identity, and then launch the session between the user and the sensor secretly, so they may communicate securely. If the gateway discovers that a user is maliciously attacking the device to steal information, it can revoke its identity.

Table 1: Security comparison

	SR-1	SR-2	SR-3	SR-4	SR-5	SR-6
Chaudhary *et al.*'s scheme [12]	✓	✗	✓	✓	✗	○
Odelu *et al.*'s scheme [9]	✓	✗	✓	✓	✗	✓
Patel *et al.*'s scheme [10]	✗	✓	✓	✓	✓	✗
The proposed scheme	✓	✓	✓	✓	✓	✓

[1] SR-1, SR-2, SR-3, SR-4 , SR-5, SR-6 represent six factors for evaluating the security and efficiency of the scheme, namely user anonymity, offline password guessing attack, mutual authentication and MITM, privilege insider attack, stolen smart card attack, revocation, respectively.
[2] ✓: The requirement is satisfied. ✗: The requirement is not satisfied or uninvolved. ○: The requirement is flawed.

SN. Sensors are generally deployed in specific fields or open environments, and they transmit the monitored and collected data to the gateway through the wireless channel. Due to the openness of the wireless channel, the transmitted content is vulnerable to malicious attacks. Sensors have limited computing, storage, and power resources. Therefore, the computation and communication cost of the sensor should be considered when designing the scheme.

USER. After the user passes the authentication of the gateway, the real-time data of the target sensor node can be obtained and controlled remotely.

3.2 Security Requirements

In the IoT environment, the exchange of information between users and gateways over wireless networks is vulnerable to a variety of attacks. Therefore, the anonymous authentication scheme should meet the following requirements.

Authentication. Anonymous authentication schemes in the IoT have to provide reciprocated authentication between the user and the gateway. The gateway must authenticate the logged-in user to ensure the user obtaining the data is legitimate. After receiving the message the gateway has sent, the user needs to verify that the information sent by the gateway has not been forged or tampered with.

Anonymous. In order to protect the user's privacy, the gateway cannot obtain the user's real identity from the messages sent by the user.

Un-linkability. Un-linkability means that the adversary cannot tell from the content of the message whether it originated from the same user. Therefore, there is no correlation between different messages sent by the same user.

Revocation. When a malicious user is found, the gateway can immediately revoke the malicious user so that it cannot establish a session secret key with the sensing device.

4 Analysis of Patel *et al.*'s RUA Scheme

4.1 Mathematical Background

An elliptic curve over a finite field $GF(p)$ is a set of all points (x, y) satisfying the equation $y^2 = (x^3 + ax + b) \bmod p$ plus a point O at infinity, where a, b, x, y are all evaluated over the finite field $GF(p)$, where p is a prime number, $(4a^3 + 27b^2) \bmod p \neq 0$. The elliptical curve is noted here as the $E_P(a, b)$.

Definition 1. *The order of a point P on $E_P(a, b)$ is the smallest positive integer satisfying $n \cdot P = P + P + \cdots + P = O$, denoted $ord(P)$, where O is the point at infinity.*

Definition 2. *Let G be a cyclic subgroup on $E_P(a, b)$ and P be a generator of G, $Q \epsilon G$. Given P and Q, find an integer m satisfying $m \cdot P = Q$, $0 \leq m \leq ord(P) - 1$, it is called the discrete logarithm problem on elliptic curves. The process of computing $m \cdot P$ is called a dot multiplication operation.*

4.2 Review of Patal *et al.*'s RUA Scheme

System Initialization Stage: The user and the gateway agree on curve $E_P()$, field q, and generator point G. Gateway chooses two random numbers k_s, $PR_{SC} \in \mathbb{Z}_P^*$ and computes $PK_s = k_s \cdot G$, $PUB_{SC} = PR_{SC} \cdot G$. k_s and PK_s are the private and public keys of the gateway, and PR_{SC} and PUB_{SC} are the private and public keys of the user, respectively. The gateway publicise PK_s and PUB_{SC}.

Registration:

1) User inputs ID, PW_i, generates $r_i \in \mathbb{Z}_P^*$, computes $B = r_i \cdot G$, $l_i = h(PW_i \parallel B)$ and forwards $\{l_i, ID\}$ to gateway via a secure channel.
2) The gateway verifies the validity of the user's identity, computes $A_i = h(h(ID) \oplus l_i)$, chooses random number $r_s \in \mathbb{Z}_P^*$, computes $S_i = r_s \cdot G$, $MID = Enc_{PK_s}(ID \parallel r_s)$, $T = h(S_i \parallel (k_s + 1))$, $O_i = T \oplus l_i$, generates the SC and stores $\{O_i, S_i, MID, A_i, h()\}$ in to it.

3) User stores $Enc_{PUB_{SC}}(B)$ in SC, SC=$(O_i, S_i, MID, A_i, h(), Enc_{PUB_{SC}}(B))$.

The Login and Authentication Phase:

1) The user inserts SC and provides ID and PW_i, computes $l_i = h(PW_i \parallel Dec_{PR_{SC}}(B))$, $A_i^* = h(h(ID) \oplus l_i)$, verifies that A_i^* is equal to A_i, chooses random number $n_p \in \mathbb{Z}_P^*$, computes $N_P = n_p \cdot G$, $T = O_i \oplus l_i$, $L_i = h(N_P \parallel ID)$, $PID = T \oplus h(ID \parallel L_i \parallel TS)$, and send $\{PID, N_P, TS, MID\}$ to the gateway.
2) Gateway gets current time TS^*, verifies that the inequality $\Delta T \leq TS^* - TS$ holds, computes $Dec_{k_s}(MID)$, $N_i = h(N_P \parallel ID)$, $T = h(r_s \parallel (k_s + 1))$, $PID^* = T \oplus h(ID \parallel N_i \parallel TS)$, then gateway verifies that the equation $PID^* = PID$ holds. If yes, gateway generates $n_s \epsilon Z_P^*$, computes $N_S = n_s \cdot G$, $SK = h(ID \parallel T \parallel n_s \cdot N_P \parallel N_S \parallel N_P)$, $SKV_i = h(SK \parallel N_S \parallel T \parallel N_P \parallel TS_{new})$. Then the gateway sends the message $\{N_S, SKV_i, TS_{new}\}$ to the user through an insecure channel.
3) User gets current time stamp TS_{new}^* and verifies that the inequality $\Delta T_{new} \leq TS_{new}^* - TS_{new}$ holds. If yes, user computes $SK^* = h(ID \parallel T \parallel n_p \cdot N_S \parallel N_S \parallel N_P)$, $Q_i^* = h(SK^* \parallel N_S \parallel T \parallel N_P \parallel TS_{new})$, verifies that Q_i^* is equal to SKV_i. If yes, user computes session key $SK = SK^*$.

4.3 Security Analysis of Patel *et al.*'s RUA Scheme

Anonymous: The RUA scheme claimed that they achieve anonymity. The user uses PID as its identity. The adversary cannot obtain the system master key to calculate the parameter T and generate a random number n_p in polynomial time. Therefore, the adversary cannot obtain the identity of the user. However, every time the user sends a message, the adversary can obtain the MID, and there is no change in the MID, the adversary can lock the target through the collected messages. Therefore, anonymity is not achieved in this scheme.

Un-linkability: Since the same user sends the same MID every time, the source of the message can be determined according to the MID. So the adversary can obtain the user's privacy and track the user.

Revocation: In the RUA scheme, there is no mention of how to revoke malicious users.

5 The Proposed Scheme

To achieve anonymous authentication and malicious user revocation in IoT, a new efficient privacy protection scheme is suggested, that consists of four phases: (1) system initialization phase, (2) user registration phase, (3) user login and identity authentication phase, (4) password update phase. Some symbols are defined in Table 2.

Table 2: Notations and description used

Notation	Descriptions
$x_{i,j}$	The j-th current private key of the user U_i
$X_{i,j}$	The j-th current public key of the user U_i
r_i	User random numbers
s	The master key of the system
P_{pub}	The public key of the system
T	Timestamp
ID	User identity
$key_{i,j}$	The j-th session key of the user U_i
PSW_i	The password of the user U_i
$Enc()/Dec()$	ECC Encryption operation and Decryption operation
v_i & $y_{i,j}$	Gateway random numbers
sk	The private key of the User
PK	The public key of the User
$PID_{i,j}$	The j-th pseudonym of the User U_i
RID_i	The real identity of U_i
$\parallel$	The message concatenation operation
$\oplus$	The exclusive-OR operation
$\rightarrow$	Insecure channel

5.1 System Initialization Stage

The system is initialized by gateway generation parameters. The gateway generates a random number $s \epsilon Z_P^*$ and computes $P_{pub} = s \cdot P$, where s and P_{pub} are the master key and public key of the system, respectively. Gateway generates a random number $sk \epsilon Z_P^*$ and computes $PK = sk \cdot P$, where sk and PK are the private key and the public key of the user, respectively. The gateway stores PK and sk in the secret memory of the user device and makes P_{pub} and PK public. Both the gateway and the user agree on curve $E_P()$, field q and generator point G.

5.2 Registration Stage

USER PART 1: User inputs ID, PSW_i and selects randomly a number $r_i \epsilon Z_P^*$, then computes $U_i = r_i \cdot P$, $w_i = h(PSW_i \parallel U_i)$, sends $\{ID, w_i\}$ to the gateway through a secure channel.

GATEWAY PART 1: The gateway verifies that the user identity is valid and then computes $TID_i = h(h(ID) \parallel w_i)$, generates a random number $v_i \epsilon Z_P^*$, Computes $V_i = v_i \cdot P$, $RID_i = Enc_{P_{pub}}(ID \parallel v_i)$, $A_i = h(V_i \parallel s)$, $B_i = A_i \oplus w_i$. Finally, gateway generates the SC which stores $\{B_i, V_i, RID_i, TID_i, h()\}$ for each user and sends the SC to user securely.

USER PART 2: The user deposits $Enc_{PK}(U_i)$ into the SC. SC=$\{B_i, V_i, RID_i, TID_i, h(), Enc_{PK}(U_i)\}$.

5.3 Login and Authentication Stage

This section mostly introduces the user login and authentication phase, where the user communicates with the gateway information via an insecure channel, as seen in Table 3.

USER PART 1: The user enters the ID, password, and inserts the SC into the card reader, which calculates $w_i = h(PSW_i \parallel Dec_{sk}(U_i))$,$TID_i^* = h(h(ID) \parallel w_i)$, then card reader verifies whether TID_i^* is equal to TID_i. If the authenticity of user is successful, SCR generates a nonce $x_{i,j}$ at random and current timestamp T. Then, SCR calculates $X_{i,j} = x_{i,j} \cdot P$, $A_i = B_i \oplus w_i$, $L_{i,j} = h(X_{i,j} \parallel ID)$, $PID_{i,j} = A_i \oplus h(ID \parallel L_{i,j} \parallel T)$, $R_{i,j} = RID_i \oplus x_{i,j} \cdot P_{pub}$. The user sends $\{PID_{i,j}, X_{i,j}, T, R_{i,j}\}$ to the gateway through an insecure channel.

GATEWAY PART 1: After receiving the massage $\{PID_{i,j}, X_{i,j}, T, R_{i,j}\}$ from user, gateway firstly checks the freshness of login request by verifying whether $\Delta T \leq T^* - T$. If it is true, gateway computes $RID_i = X_{i,j} \cdot s \oplus R_{i,j}$, $Dec_s(RID_i)$, $N_i = h(X_{i,j} \parallel ID)$, $A_i = h(v_i \parallel s)$, $PID_{i,j}^* = A_i \oplus h(ID \parallel N_i \parallel T)$, and checks whether $PID_{i,j}^*$ is equal to $PID_{i,j}$ to authenticate the authenticity of user. If it holds, gateway then randomly generates a nonce $y_{i,j} \epsilon Z_P^*$ and the current timestamp T_{new}. Gateway also computes $Y_{i,j} = y_{i,j} \cdot P$, $key_{i,j} = h(ID \parallel A_i \parallel y_{i,j} \cdot X_{i,j} \parallel Y_{i,j} \parallel X_{i,j})$, $SKV_i = h(key_{i,j} \parallel Y_{i,j} \parallel A_i \parallel X_{i,j} \parallel T_{new})$. Gateway sends $\{Y_{i,j}, SKV_i, T_{new}\}$ to the user over an open channel.

USER PART 2: Upon receiving broadcast message, user firstly checks the freshness of message by verifying $\Delta T_{new} \leq T_{new}^* - T_{new}$. If the inequality holds, user computes $key_{i,j}^* = h(ID \parallel A_i \parallel x_{i,j} \cdot Y_{i,j} \parallel Y_{i,j} \parallel X_{i,j})$ to verifies the session key $key_{i,j}^*$ and gateway. Then user computes $Q_i^* = h\left(key_{i,j}^* \parallel Y_{i,j} \parallel A_i \parallel X_{i,j} \parallel T_{new}\right)$ and checks whether $Q_i^* = SKV_i$. If so, session key is established successfully.

5.4 Password Update Stage

During this phase, an authorised user can update the password using the ensuing steps without a gateway being involved.

USER PART 1: User firstly inserts SC to the card-reader and inputs the personal credentials such as ID, PSW_i, $PSW_i^{'}$.

SCR PART 1: SCR computes $Dec_{sk}(U_i)$ to get U_i, computes $w_i = h(PSW_i \parallel U_i)$, $TID_i^* = h(h(ID) \parallel w_i)$, and checks whether TID_i^* is equal to TID_i to authenticate the authenticity of user. If it holds, gateway then randomly generates a nonce $r_i^{'} \epsilon Z_P^*$ and computes $U_i^{'} = r_i^{'} \cdot P$, $w_i^{'} = h\left(PSW_i^{'} \parallel U_i^{'}\right)$, $B_i^{'} = w_i \oplus w_i^{'} \oplus B_i$, $TID_i^{'} = h\left(h(ID) \parallel w_i^{'}\right)$. Now SCR generates updated SC=$\left(B_i^{'}, V_i, RID_i, TID_i^{'}, h(), Enc_{PK}\left(U_i^{'}\right)\right)$.

6 Security Analysis and Performance Evaluation

This section analyses the performance of the proposed scheme by making a comparison with the existing schemes of Chaudhary *et al.* [12] , Odelu *et al.* [9]and Patel *et al.* [10]The security proof and analysis of the proposed scheme are presented, along with a demonstration that it satisfies the security and privacy requirements of IoT.

6.1 Proof

In this subsection, we will discuss the validity of the mutual authentication equation between the user and the gateway.

When the user received the message $< Y_{i,j}, SKV_i, T_{new} >$, then the following equation will be verified:

$$Q_i^* = SKV_i$$

If the message is legal, then the following equation can be derived:

$$\begin{aligned} Q_i^* &= h(key_{i,j}^* \parallel Y_{i,j} \parallel A_i \parallel X_{i,j} \parallel T_{new}) \\ &= h(h(ID \parallel A_i \parallel x_{i,j} \cdot Y_{i,j} \parallel Y_{i,j} \parallel X_{i,j}) \parallel Y_{i,j} \parallel A_i \parallel X_{i,j} \parallel T_{new}) \\ &= h(h(ID \parallel A_i \parallel x_{i,j} \cdot P \cdot y_{i,j} \parallel Y_{i,j} \parallel X_{i,j}) \parallel Y_{i,j} \parallel A_i \parallel X_{i,j} \parallel T_{new}) \\ &= h(key_{i,j} \parallel Y_{i,j} \parallel A_i \parallel X_{i,j} \parallel T_{new}) \\ &= SKV_i \end{aligned}$$

Therefore, the proposed scheme can achieve mutual authentication between the user and the gateway, and guarantee the anonymity and un-linkability of the user.

6.2 Security Analysis

In the subsection,we will analyze the security and privacy of our scheme.

Anonymity and Un-linkability: In this scheme, each message sent by a user is encrypted with a random number. The hash function and XOR operation is used to generate the pseudonym of the user. It is impossible for an adversary A to get the gateway secret key to calculate the parameter T, so it is impossible for an adversary A to calculate the user ID. We use the public key of the system and the random number $x_{i,j}$ to encrypt the real identity RID_i of the U_i to generate the parameter $R_{i,j}$, so the adversary A cannot judge the source of the message is the same

Table 3: Proposed scheme: login and authentication phases

User/SCR		Gateway
The Login and Authentication Phase: Enters SC and provides ID and PSW_i , Computes $w_i = h\left(PSW_i \parallel Dec_{sk}\left(U_i\right)\right)$, Computes $TID_i^* = h\left(h\left(ID\right) \parallel w_i\right)$, Verifies $TID_i^* \stackrel{?}{=} TID_i$ Generates $x_{i,j} \epsilon Z_P^*$, Computes $X_{i,j} = x_{i,j} \cdot P$, Computes $A_i = B_i \oplus w_i$, Computes $L_{i,j} = h\left(X_{i,j} \parallel ID\right)$, Computes $PID_{i,j} = A_i \oplus h\left(ID \parallel L_{i,j} \parallel T\right)$, Computes $R_{i,j} = RID_i \oplus x_{i,j} \cdot P_{pub}$.	$\xrightarrow{\{PID_{i,j}, X_{i,j}, T, R_{i,j}\}}$	
		Gets current timestamp T^*, Verifies $\triangle T \stackrel{?}{\leq} T^* - T$, Computes $RID_i = X_{i,j} \cdot s \oplus R_{i,j}$, Computes $Dec_s\left(RID_i\right)$, Computes $N_i = h\left(X_{i,j} \parallel ID\right)$, Computes $A_i = h\left(v_i \parallel s\right)$, Computes $PID_{i,j}^* = A_i \oplus h\left(ID \parallel N_i \parallel T\right)$, Computes $PID_{i,j}^*$ is equal to $PID_{i,j}$, Generates $y_{i,j} \epsilon Z_P^*$, Computes $Y_{i,j} = y_{i,j} \cdot P$, Computes $key_{i,j} = h\left(ID \parallel A_i \parallel y_{i,j} \cdot X_{i,j} \parallel Y_{i,j} \parallel X_{i,j}\right)$, $SKV_i = h\left(key_{i,j} \parallel Y_{i,j} \parallel A_i \parallel X_{i,j} \parallel T_{new}\right)$.
	$\xleftarrow{\{Y_{i,j}, SKV_i, T_{new}\}}$	
Gets current timestamp T_{new}^*, Verifies $\triangle T_{new} \stackrel{?}{\leq} T_{new}^* - T_{new}$, Computes $key_{i,j}^* = h\left(ID \parallel A_i \parallel x_{i,j} \cdot Y_{i,j} \parallel Y_{i,j} \parallel X_{i,j}\right)$, $Q_i^* = h\left(key_{i,j}^* \parallel Y_{i,j} \parallel A_i \parallel X_{i,j} \parallel T_{new}\right)$, Verifies $Q_i^* \stackrel{?}{=} SKV_i$, if yes, computes session key $key_{i,j} = key_{i,j}^*$.		

user. Therefore, the scheme satisfies anonymity and Un-linkability.

Traceability: The message tuple $\{PID_{i,j}, X_{i,j}, T, R_{i,j}\}$ that sent by the user, gateway can calculate $RID_i = X_{i,j} \cdot s \oplus R_{i,j}$, where s is the master key of the system. Therefore, gateway can get the real identity RID_i of the U_i.

Revocation: The gateway has a CRL that stores the malicious user information. The misbehaving user can be deleted from the network through the CRL, and the session key cannot be established with the sensing device.

6.3 Performance Evaluation

Computation Cost: This section compares the computational costs of the four schemes, and some notations used in this section are defined as follows:

T_H**:** The running time to execute the hash function.

T_{pa}**:** The running time for performing elliptic curve point addition.

T_{pm}**:** The running time for performing elliptic curve point multiplication.

T_{Sym}**:** The time at which encryption and decryption are performed in a symmetric encryption algorithm.

Table 4: Comparison of computation cost

Schemes	User computation (ms)
Chaudhary *et al.* [12]	$5T_H+4T_{pm} \approx 8.9155$
Odelu *et al.* [9]	$7T_H+3T_{pm}+1T_{Sym} \approx 6.6987$
Patel *et al.* [10]	$6T_H+2T_{pm}+1T_{Sym} \approx 4.4704$
The proposed scheme	$6T_H+3T_{pm}+1T_{Sym} \approx 6.6964$

The experiment for the IoT is conducted on an Intel x86-64 processor at Intel (R) Core (TM) i5-7500 CPU with 3.40 GHz. According to Patel *et al.*'s [10] experiment, the running time of T_H, T_{pa}, T_{pm}, T_{Sym} are 0.0023 ms, 0.028 ms, 2.226 ms, 0.0046 ms respectively. The client has restricted computing capacity and memory, but the gateway has ample resources to compute and store. Consequently, the computational cost is compared on the client side. In Chaudhary *et al.*'s [12] security-enhanced scheme, the user computes five hash function operations, four elliptic curve point multiplication operations. The user's computation cost is $5T_H+4T_{pm} \approx 8.9155$ ms. In Odelu *et al.*'s [9] authentication scheme, the user computes seven hash function operations, three elliptic curve point multiplication operations and one symmetric encryption operation. The user's computation cost is $7T_H+3T_{pm}+1T_{Sym} \approx 6.6987$ ms. In Patel *et al.*'s [10] scheme, the user computes six hash function operations, two elliptic curve point multiplication operations and one symmetric encryption operation. The user's computation cost is $6T_H+2T_{pm}+1T_{Sym} \approx 4.4704$ ms. In our scheme, the user computes six hash function operations, three elliptic curve point multiplication operations and one symmetric encryption operation. The user's computation cost is $6T_H+3T_{pm}+1T_{Sym} \approx 6.6964$ ms. Compared with the scheme of Patel *et al.* [10], although the computational cost of this scheme is not the lowest, it does have sufficient reliability compared with other schemes. The computational costs of the four schemes are listed in Table 4.

Communication Cost: Communication cost refers to the number of bits communicated before the session key is established. According to the scheme of Patel *et al.* [10], the hash output is 160 bits. The size of the timestamp is 32 bits. The size of the randomly generated primary sequence is 128 bits. The size of each coordinate in ECC is 160 bits, so the size of each point is 320 bits. Therefore, the private key is 160 bits and the public key is 320 bits. Table 5 shows the comparison results of the communication costs of all schemes.

Table 5: Comparison of communication cost

Schemes	Messages	Cost (bits)
Chaudhary *et al.*'s scheme [12]	2	1344
Odelu *et al.*'s scheme [9]	3	1600
Patel *et al.*'s scheme [10]	2	800
The proposed scheme	2	800

7 Conclusion

Patel *et al.* [10] proposed a two-factor authentication scheme based on the user-gateway communication model, which were user identity, password and smart card, but the scheme did not have anonymity and message unlinkability. This paper proposed a secure and effective conditional privacy protection scheme based on ECC. After successful registration, the user enters the login phase. The user ID is encrypted with the system public key and the random number generated by the user's device, and sent to the gateway for mutual authentication between the user and gateway. The secure session key is then generated. In addition, a revocation mechanism is added to the scheme. Although the computational cost is a little higher than Patel *et al.*'s [10] scheme, the proposed scheme provides a good balance between security and efficiency.

Acknowledgments

This research was supported by the Natural Science Research Key Project of Colleges and Universities in Anhui Province (No.2022AH050874) , Project of Excellent and Top-notch Talent Cultivation of Anhui Province University (gxbjZD2022087) and Talent Founda-tion of agricultural university (rc482005).

References

[1] F. Al-Turjman and S. Alturjman, "Context-sensitive access in industrial internet of things (iiot) healthcare applications," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2736–2744, 2018.

[2] R. H. Aswathy and N. Malarvizhi, "A design of lightweight ecc based cryptographic algorithm coupled with linear congruential method for resource constraint area in iot," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–10, 2021.

[3] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic id-based remote user authentication scheme," *IEEE transactions on Consumer Electronics*, vol. 50, no. 2, pp. 629–631, 2004.

[4] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks," *IEEE transactions on industrial informatics*, vol. 15, no. 9, pp. 4957–4968, 2019.

[5] S. K. Islam and M. K. Khan, "Cryptanalysis and improvement of authentication and key agreement protocols for telecare medicine information systems," *Journal of medical systems*, vol. 38, no. 10, pp. 1–16, 2014.

[6] M. K. Khan, S.-K. Kim, and K. Alghathbar, "Cryptanalysis and security enhancement of a 'more efficient

& secure dynamic id-based remote user authentication scheme'," *Computer Communications*, vol. 34, no. 3, pp. 305–309, 2011.

[7] X. Li, J. Niu, Z. A. Bhuiyan, F.n Wu, M. Karuppiah, and S. Kumari, "A robust ecc-based provable secure authentication protocol with privacy preserving for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3599–3609, 2017.

[8] S. K. Mousavi, A. Ghaffari, S. Besharat, and H. Afshari, "Security of internet of things based on cryptographic algorithms: a survey," *Wireless Networks*, vol. 27, pp. 1515–1555, 2021.

[9] V Odelu, A K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," *IEEE Transactions on information forensics and Security*, vol. 10, no. 9, pp. 1953–1966, 2015.

[10] C. Patel and N. Doshi, "Secure lightweight key exchange using ecc for user-gateway paradigm," *IEEE Transactions on Computers*, vol. 70, no. 11, pp. 1789–1803, 2020.

[11] S. Qiu, G. Xu, H. Ahmad, and L. Wang, "A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems," *IEEE access*, vol. 6, pp. 7452–7463, 2017.

[12] T. Shon M. Sher S. A. Chaudhry, H. Naqvi and M. S. Farash, "Cryptanalysis and improvement of an improved two factor authentication protocol for telecare medicine information systems," *CoRR abs/1607.01471*, 2016.

[13] Y. Su, G. Shen, and M. Zhang, "A novel privacy-preserving authentication scheme for v2g networks," *IEEE Systems Journal*, vol. 14, no. 2, pp. 1963–1971, 2019.

[14] S. Velliangiri, R. Manoharn, S. Ramachandran, K. Venkatesan, V. Rajasekar, P. Karthikeyan, P. Kumar, A. Kumar, and S. S. Dhanabalan, "An efficient lightweight privacy-preserving mechanism for industry 4.0 based on elliptic curve cryptography," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6494–6502, 2021.

[15] R. Vinoth, L. J. Deborah, P. Vijayakumar, and N. Kumar, "Secure multifactor authenticated key agreement scheme for industrial iot," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3801–3811, 2020.

[16] Y. Y. Wang, J. Y. Liu, F. X. Xiao, and J. Dan, "A more efficient and secure dynamic id-based remote user authentication scheme," *Computer communications*, vol. 32, no. 4, pp. 583–585, 2009.

[17] J. Wei, T. V. X. Phuong, and G. Yang, "An efficient privacy preserving message authentication scheme for internet-of-things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 617–626, 2020.

[18] H. L. Wu, C. C. Chang, Y. Z. Zheng, L. S. Chen, and C. C. Chen, "A secure iot-based authentication system in cloud computing environment," *Sensors*, vol. 20, no. 19, p. 5604, 2020.

[19] X. Xu, P. Zhu, Q. Wen, Z. Jin, H. Zhang, and L. He, "A secure and efficient authentication and key agreement scheme based on ecc for telecare medicine information systems," *Journal of medical systems*, vol. 38, no. 1, pp. 1–7, 2014.

Biography

Mana Mao is a student at the School of Information and Computer Science, Anhui Agricultural University. Her research interest is Internet of Things security in wireless communication.

Jiujiu Yu is now a Professor in the School of Computer Engineering, Anhui Sanlian University. He received MSE degree in Zhejiang University in 2007. His research interests include agile software testing, software project management, etc.

Yimin Wang is now an Associate Professor in the School of Computer Science and Technology, Anhui Agriculture University. He received PhD degree in Anhui University of China in 2017. His research interests include security and privacy for wireless networks, cloud computing, big data, etc.

Study on Encryption Protection of User Privacy Data in the Logistics Industry from a Legal Perspective

Can Wei

(Corresponding author: Can Wei)

College of Marxism, Henan Vocational University of Science and Technology
No. 6, East Section of Wenchang Avenue, Zhoukou, Henan 466000, China
cau404680@163.com

(Received May 12, 2022; Revised and Accepted May 23, 2023; First Online June 25, 2023)

Abstract

There is legal support for the protection of logistics users' privacy information. This paper briefly described the legal basis for protecting logistics users' privacy information, proposed a logistics users' privacy data encryption model that combines blockchain to meet enterprises' and individuals' legal and everyday needs for privacy data protection, and then conducted simulation experiments on the model. The results showed that the blockchain database in the encryption model could effectively prevent the leakage of users' privacy information; the identity-based segmented encryption algorithm used in the model had higher encryption and decryption efficiency than the traditional encryption algorithm; sites with different permissions only queried partial information of users based on logistics numbers, while sites without permissions only queried a garbled string.

Keywords: Legal Perspective; Logistics; User Privacy

1 Introduction

Logistics industry is an important part of modern economy. Internet companies such as Alipay have also entered the logistics field. Big data analysis, artificial intelligence and other technical means have improved the ability to collect and process logistics information [11], but at the same time, the use, protection, and privacy of logistics information have been paid attention to. In the logistics industry, the encryption and protection of users' personal information has been supported by certain laws, so logistics enterprises need to strengthen the protection [3] and introduce encryption technology to protect users' privacy. In addition, despite the law's support for users' privacy information protection in the logistics sector, the existing law still has shortcomings. After the leakage of user privacy information, it is difficult to be held accountable, and the punishment (compensation) is light, so there is also a demand for logistics users [8].

The relevant studies are listed below. Zhang *et al.* [15] proposed and demonstrated the secrecy of a two-dimensional encrypted code-based logistics information privacy protection system. On the basis of encrypted two-dimensional code, Qi *et al.* [5] created a fast management system and tested its effectiveness. A dynamic data encryption approach was developed by Gai *et al.* [4] with the goal of maximizing the scope of privacy protection while adhering to the necessary execution time. This paper briefly described the legal basis of logistics user privacy information protection, proposed a logistics user privacy data encryption model combined with blockchain to meet the needs of enterprises and individuals in terms of privacy data protection in laws and daily life, and then simulated the model.

2 Logistics User Privacy from a Legal Perspective

With the development of the e-commerce industry, the logistics and express delivery industry has also risen and gradually become an important part of social and economic development. In order to effectively deter and curb illegal activities based on logistics, the real-name system for logistics has been gradually implemented [14]. In addition to the above functions, the real-name system for logistics can regulate the management rules of the logistics industry, and for users, the real-name system can provide effective support for safeguarding their legitimate rights and interests. However, the real-name system for logistics also has its disadvantages. The real-name system means that the user's personal information presented in the logistics process is true and reliable, but it is not controlled by the individual user in the logistics process, and the in-

terlocking logistics services have also increased the risk of personal information leakage [12].

There are approximately 40 laws and 200 regulations and systems that are related to the protection of users' personal information in logistics. For example, the "Cybersecurity Law of the People's Republic of China" stipulates the protection standards, responsibility sharing, and special specifications in key areas for personal information; the "Personal Information Protection Law of the People's Republic of China" specifies in detail how personal information can be collected, used, stored, and deleted, and includes related terms for confidential, secure, and lawful processing of personal information; the "E-commerce Law of the People's Republic of China" stipulates the requirements for electronic commerce platforms to ensure the security of consumers' personal information and protect their privacy; and the "Industry Management Regulations of the People's Republic of China" strengthens the privacy protection rules for all kinds of information entities according to the needs of different industries and organizations [10].

On the whole, there are many legal regulations for logistics users' personal information, which provide legal protection for enterprises and individuals to protect their personal information. However, due to the large number and level of laws, these regulations are not systematic and scattered, and the content regulations are relatively general, mostly in the form of policy regulations to cover as many areas as possible. Finally, accountability is unclear and the burden of proof is high when pursuing accountability; the existing laws are lighter in punishment for violating personal information than the benefits obtained from the violation; and different regulatory departments follow different regulations, which lack coordination [13].

3 Modeling Algorithms for Privacy Data Protection

The previous text briefly described the protection of logistics users' privacy from a legal perspective. It can be seen from the description that logistics personal information is protected by many legal regulations, but there are also shortcomings. Due to the existence of legal provisions for the privacy of logistics users' personal information, logistics businesses are required to take user privacy protection seriously throughout the logistical process, while the shortcomings of the legal provisions have caused users to have the need to protect personal information in this process. This user demand may also drive logistics providers to give user privacy protection more consideration.

Figure 1 shows the flow of the logistics user privacy data encryption model incorporating blockchain [6], which uses the hierarchical identity encryption algorithm to encrypt user privacy data, and uses blockchain to ensure the authenticity of the encrypted privacy data in the transmission process. The specific steps are described below.

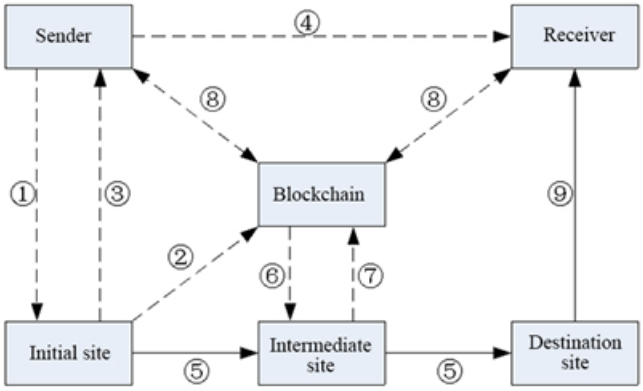


Figure 1: Flow of the logistics user privacy data encryption model combined with blockchain

1) The sender gives the package to be sent to the initial site and provides relevant receiver information, including the address, name and contact information.

2) After the initial site combines the received recipient information and the address information of the initial site, the combined information is encrypted in segments. The encryption formula is:

$$\begin{aligned} P_t &= H_1(id_1, id_2, \cdots, id_t) \\ \sigma &\in \{0,1\}^n \\ r &= H_3(\sigma, m) \\ Y_t &= s_t \epsilon \\ c &= [r\epsilon, \sigma \oplus H_2(e(rY_{t-1}, P_t)), m \oplus H_4(\sigma)] \end{aligned}$$

where id_t is the identity level information of different segments [9] (the number of t depends on the number of segments of the combined information), σ is a random number, r is the parameter obtained from σ and plaintext m after the calculation using the hash function $H_3 : \{0,1\}^n \times \{0,1\}^n \in Z_q^*$, c is the ciphertext after segment encryption, s_t is the random number of the t-th identity level, ϵ and e are public parameters, and $H_1(\cdot)$, $H_3(\cdot)$, and $H_4(\cdot)$ are all hash functions. The encrypted ciphertext is verified by the smart contract [1] of the blockchain and then stored in the blockchain, and a tracking number is generated.

3) The initial site returns the tracking number to the sender.

4) The sender returns the tracking number back to the receiver.

5) Parcels are transported through the intermediate site to the destination site.

6) During the transportation of the parcel, the intermediate site queries the corresponding address ciphertext from the blockchain through the tracking number, and decrypts the ciphertext through the private

key of the corresponding level owned by the intermediate site, so as to obtain the plaintext of the address of the next site. The decryption formula is:

$$\begin{aligned} c &= [r\epsilon, \sigma \oplus H_2(e(rY_{t-1}, P_t)), m \oplus H_4(\sigma)] \\ &= [U, V, W] \\ \sigma &= V \oplus H_2(e(U, sk_t)) \\ m &= W \oplus H_4(\sigma) \end{aligned}$$

where sk_t is the private key of the corresponding level that the intermediate site has.

7) The logistics information of the parcel arriving at that intermediate site are uploaded to the blockchain.

8) The sender and the receiver can check the logistics information of the parcel from the blockchain according to the tracking number.

9) The last site also uses the tracking number and the private key of the corresponding level of the site to decrypt the ciphertext, so as to obtain the name and contact information of the receiver, and send a short message to notify the receiver come to pick up the parcel [2].

4 Simulation Experiments

4.1 Experimental Environment

The simulation experiments were conducted on a server in the laboratory. The logistic user privacy data encryption model used in this paper used blockchain technology, and the required blockchain network was provided by the virtual machine of Ethernet [7]. The server in the laboratory was equipped with quad-core i7 CPU, 16 G memory, and 1,024 G hard disk. The parameters of the virtual machine provided by Ethernet were uniformly set to single-core i5 CPU, operating frequency 2.5 GHz, and memory 4 G for the sake of simulation. The number of nodes provided by the virtual machine was 5.

4.2 Experimental Projects

Project (1): Testing the security of the encryption model for storing user information
First, ten sets of logistics users' privacy information were randomly generated, including users' names, contact information, and addresses. These ten sets of information were then stored in both a traditional central database and a blockchain database. The traditional central database was provided by a local server in the laboratory. To facilitate queries, the traditional database stored the privacy data in plaintext and protected the data by setting access permissions. The blockchain database was provided by Ethereum virtual machine nodes, and the data was protected by the blockchain network.
Finally, a third-party server was used to perform a hacker attack on both databases, bypassing the access permissions to access the data in the databases. The access results of the two databases were compared.

Project (2): Testing the efficiency of segmented encryption algorithms
The ten randomly generated pieces of personal information mentioned above were encrypted. For comparison, the traditional whole-segment encryption algorithm was also used to encrypt the entire personal information using a single key pair. The efficiency of the two encryption methods was tested under different numbers of pieces of personal information.

Project (3): Testing the logistics user privacy encryption model for the protection of privacy information during the logistics process
The logistics delivery process was simulated using servers and a blockchain network in the laboratory. First, the three servers were designated as the initial site, intermediate site, and destination site. The initial site first encrypted and uploaded ten randomly generated pieces of personal information onto the chain, and printed out the corresponding delivery documents with tracking numbers, while hiding key personal information. The intermediate and destination sites then queried the tracking number. In addition to the normal queries from authorized intermediate and destination sites, the tracking number was also queried by a fourth server without proper authorization.

4.3 Experimental Results

Table 1 shows the data stored in two databases obtained from a third-party server using hacking techniques to bypass access permissions. The results of illegal access to traditional databases contained complete user privacy information, while the results of illegal access to blockchain databases contained only a series of numbers and no clear user privacy information. This indicates that if traditional databases are successfully attacked by hackers, their internal user privacy information will be directly leaked, while even if blockchain databases are illegally accessed by hackers, the privacy information in their databases has been encrypted using the hash algorithm, and only the ciphertext will be directly leaked, and the privacy information contained in the plaintext will not be leaked.

Figure 2 shows the efficiency of the traditional encryption algorithm and the segmented encryption algorithm when dealing with different amounts of personal information. As shown in Figure 2, as the amount of personal information to be encrypted increased, the time required to encrypt and decrypt increased for both algorithms. For the same amount of personal information, the time required to encrypt and decrypt using the traditional al-

Table 1: The access results of illegal access to the two databases

	Traditional Database			Blockchain Database		
	Name	Contact Information	Delivery address	Name	Contact Information	Delivery Address
User 1	Zhang San	14785236955	No. 1, District B, City A	12368457	32658774	45687412
User 2	Li Si	12365897458	No. 2, District C, City B	23659854	74548256	34538545
User 3	Wang Wu	13569874589	No. 3, District D, City C	25748964	64584318	34475368
User 4	Ma Liu	14785236958	No. 6, District C, City D	12546468	25587468	54545121
User 5	Zhao Yi	12574786489	No. 8, District A, City E	64465845	26648546	35647825
User 6	Qian Er	13659955647	No. 7, District B, City F	35969324	12425354	75462231
User 7	Sun San	15897965485	No. 9, District E, City G	32684824	34526845	24582665
User 8	Zhou Qi	16986359474	No. 5, District A, City H	36494156	45526746	52254577
User 9	Wu Ba	14789635845	No. 3, District C, City I	68475856	34584627	45465565
User 10	Zheng Jiu	19887554122	No. 4, District D, City J	25876456	34672446	32554484

gorithm was greater than the time using the segmented encryption algorithm. The reason for this is as follows. As the amount of personal information increased, the number of strings that the encryption algorithm must encrypt increased, and thus the amount of time needed to encrypt and decrypt also increased. The traditional encryption algorithm used a pair of keys to encrypt and decrypt the entire personal information, while the segmented encryption algorithm divided the personal information into shorter segments and encrypted and decrypted each segment in parallel using a pair of keys, resulting in less time.

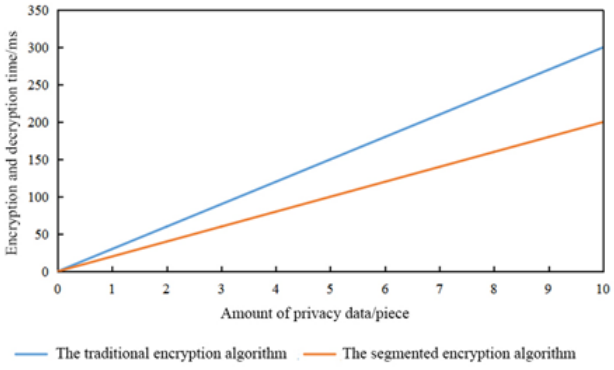


Figure 2: Efficiency of two encryption algorithms when facing different amounts of private data

Table 2 shows the results obtained by different authorized sites using tracking numbers when simulating the logistics process in the laboratory. The intermediate site is an intermediate transition during the logistics transportation process, and its authorization key can only allow it to query the next level of site, and cannot query the previous level site or other information. This is also reflected in the results shown in Table 2, where the query results of the intermediate site were only limited to a specific district. The authorization key of the destination site can only query the user name and contact information, and this is also reflected in the results shown in Table 2. Even if an unauthorized site knows the tracking number, the result of its query will only be a garbled output, as displayed in Table 2.

5 Discussion

The logistics industry is an important part of the modern economy, and often involves a significant amount of personal privacy information during the transportation process. Once personal privacy information is used by illegal individuals, it can cause serious losses. Therefore, personal privacy information security is critical in logistics. This article first briefly introduced the protection of personal privacy information from a legal perspective. At present, China has relatively more legal regulations for logistics users' personal information, which provides legal protection for enterprises and individuals to protect personal privacy information. However, there are still some challenges due to the vague and broad wording of the regulations, resulting in loopholes in the regulatory process. This creates disadvantages for logistics users in terms of unclear responsibilities, difficulties in proving their case, and high costs in defending their rights. This article therefore makes a number of proposals.

1) The government should further improve the laws and regulations on the protection of logistics privacy information and integrate and clarify the fragmented and overlapping regulations to clearly define the rights and responsibilities in the logistics process, avoid general principles and guidelines, and increase the punishment for violations.

2) The government should strengthen enforcement supervision, clarify the responsibilities and authority of relevant logistics departments, avoid overlapping functions, and establish coordination mechanisms to strengthen information flow.

Table 2: Query results of user privacy information by different authorized sites

User number	Tracking number	The search result of the intermediate site	Target site search results	The research result of the unauthorized site
User 1	20230215001	Area B	Zhang San; 14785236955	F68a7468a4
User 2	20230215002	Area C	Li Si; 12365897458	A5faf5a44f6
User 3	20230215003	Area D	Wang Wu; 13569874589	A56f46a4f6d
User 4	20230215004	Area C	Ma Liu; 14785236958	Afa7468f4f54
User 5	20230215005	Zone A	Zhao Yi; 12574786489	5a4a4aa464f
User 6	20230215006	Area B	Qian Er; 13659955647	Fa4f68545fa6
User 7	20230215007	Zone E	Sun San; 15897965485	65468a4f6a4
User 8	20230215008	Zone A	Zhou Qi; 16986359474	A45f4a45354
User 9	20230215009	Area C	Wu Ba; 14789635845	Daf4wf134s6
User 10	20230215010	Area D	Zheng Jiu; 19887554122	Gqa4fga5a84

3) The government should regulate the operation of the logistics industry and encourage the industry to develop encryption schemes that can protect the privacy of logistics users, while promoting self-regulation and restriction.

In the following sections, this article provided a detailed introduction of a logistics user privacy data encryption model combined with blockchain to satisfy the needs of companies and users for privacy protection at the legal and everyday levels. Finally, the privacy data encryption model was verified through simulation experiments. It was found that the encryption model could effectively protect users' private data in the database and protect users' privacy during the logistics delivery process.

6 Conclusion

In this article, the legal basis for protecting logistics users' privacy information was briefly described, and a logistics users' privacy data encryption model combined with blockchain was proposed to meet the needs of enterprises and individuals for privacy data protection at the legal and everyday levels. The model was then verified through simulation experiments. The obtained results are as follows.

1) The traditional centralized database leaked users' privacy data after illegal access, while the blockchain database leaked only ciphertext data and not users' privacy data.

2) Compared with the traditional encryption algorithm, the segmented encryption algorithm was more efficient in encryption and decryption.

3) In the logistics simulation process, different authorized sites only queried the corresponding user information with their specific permissions based on the tracking number, while unauthorized sites only received a garbled output.

References

[1] Y. Aono, T. Hayashi, L. T. Phong, L. Wang, "Privacy-preserving logistic regression with distributed data sources via homomorphic encryption," *IEICE Transactions on Information & Systems*, vol. E99.D, no. 8, pp. 2079-2089, 2016.

[2] A. Chadha, S. Mallik, A. R. Chadha, R. Johar, M. M. Roja, "Dual-layer video encryption using RSA algorithm," *International Journal of Computer Applications*, vol. 116, no. 1, pp. 33-40, 2015.

[3] K. F. Cheung, M. G. H. Bell, J. Bhattacharjya, "Cybersecurity in logistics and supply chain management: An overview and future research directions," *Transportation Research Part E Logistics and Transportation Review*, vol. 146, no. February, pp. 1-18, 2021.

[4] K. Gai, M. Qiu, H. Zhao, J. Xiong, "Privacy-aware adaptive data encryption strategy of big data in cloud computing," in *IEEE International Conference on Cyber Security & Cloud Computing*, pp. 273-278, 2016.

[5] Q. Han, C. Du, Y. Yao, L. Lei, "A new express management system based on encrypted QR code," in *8th International Conference on Intelligent Computation Technology and Automation (ICICTA'15)*, pp. 53-56, 2015.

[6] Z. Hua, Y. Zhou, C. M. Pun, C. L. P. Chen, "2D sine logistic modulation map for image encryption," *Information Sciences*, vol. 297, no. C, pp. 80-94, 2015.

[7] G. Iovane, A. Amorosia, E. Benedetto, G. Lamponi, "An information fusion approach based on prime numbers coming from RSA algorithm and Fractals for secure coding," *Journal of Discrete Mathematical Sciences & Cryptography*, vol. 18, no. 5, pp. 455-479, 2015.

[8] K. Lee, I. Kim, S. O. Hwang, "Privacy preserving revocable predicate encryption revisited," *Security & Communication Networks*, vol. 8, no. 3, pp. 471-485, 2015.

[9] Y. Liu, S. Tang, R. Liu, L. Zhang, Z. Ma, "Secure and robust digital image watermarking scheme using logistic and RSA encryption," *Expert Systems with Applications*, vol. 97, pp. 95-105, 2018.

[10] N. Martindale, S. L. Stewart, N. A. Mcgirl, M. B. Adams, G. Westphal, J. R. Garner, "Enabling computation on sensitive data in international safeguards with privacy-preserving encryption techniques," *Journal of nuclear Materials Management*, vol. 49, no. 2, pp. 16-25, 2021.

[11] J. Ouyang, X. Chen, "Personal information two-dimensional code encryption technology in the process of e-commerce logistics transportation," *SAIEE Africa Research Journal*, vol. 113, no. 1, pp. 52-57, 2022.

[12] J. L. Raisaro, G. Choi, S. Pradervand, R. Colsenet, N. Jacquemont, N. Rosat, V. Mooser, J. P. Hubaux, "Protecting privacy and security of genomic data in i2b2 with homomorphic encryption and differential privacy," *IEEE/ACM Transactions on Computational Biology & Bioinformatics*, vol. 15, no. 5, pp. 1413-1426, 2017.

[13] X. A. Wang, F. Xhafa, W. Cai, J. Ma, F. Wei, "Efficient privacy preserving predicate encryption with fine-grained searchable capability for cloud storage," *Computers & Electrical Engineering*, vol. 56, pp. 871-883, 2016.

[14] X. Yan, S. Zhuo, Y. Wu, B. Chen, "Distributed privacy-preserving fusion estimation using homomorphic encryption," *Journal of Beijing University of Technology*, vol. 31, no. 6, pp. 551-558, 2022.

[15] X. Zhang, H. Li, Y. Yang, G. Sun, G. Chen, "LIPPS: Logistics information privacy protection system based on encrypted QR code," in *IEEE Trustcom/BigDataSE/I SPA*, pp. 996-1000, 2016.

Biography

Can Wei, born in December 1980, has received a master's degree. She is a lecturer and is working in Henan Vocational University of Science and Technology. She interested in criminal law.

Public Data Integrity Auditing Scheme Based on Fuzzy Identity for Cloud Storage System

Yilin Yuan[1], Yifan Gu[2], and Zhenzhen Zhang[1]
(Corresponding author: Yilin Yuan)
College of Information Engineering, Beijing Institute of Graphic Communication[1]
Beijing 102600, China
College of Electronic Engineering, South China Agricultural University, Guangzhou, China[2]
Email: yuanyilin@bigc.edu.cn; guyifan@stu.scau.edu.cn; zhangzhenzhen@bigc.edu.cn
(Received Nov. 28, 2022; Revised and Accepted May 12, 2023; First Online June 25, 2023)

Abstract

Recently, some integrity verification schemes used unique biometric data as the cryptographic private key, it's convenient, but the file tags are related to the number of feature vectors which will incur additional costs. So, this paper proposes a public data integrity auditing scheme based on fuzzy identity. A new method named Fuzzy Identity Processing (FIP) is provided to obtain the user's private key. FIP takes the feature vectors extracted from the user's biometric data as input and outputs the user identity. The valid identity helps generate a private key and calculates the file's tags set. Significantly, the tags set is irrelevant to the number of feature vectors. And this design will significantly reduce the computational overhead and storage space. Moreover, authorized users can view the audit result in the audit phase. The scheme's security is strictly proven, and performance evaluation demonstrates that it is feasible and effective.

Keywords: Cloud Security Storage; Data Integrity; Fuzzy Identity; Public Auditing

1 Introduction

With the popularity of cloud computing, cloud storage is widely used. Cloud storage is a cloud computing system with data storage and management as its core, which is essentially a service. In recent years, more and more users have chosen to used cloud storage services. Cloud storage adopts network online storage mode. It archives, organizes, and distributes data from different physical hardware on demand to multiple virtual servers hosted by a third party. Cloud storage has many advantages: (1) Pay on-demand; it means that the user subscribes to different storage services according to the amount of data. (2) Users do not need to deploy physical storage devices locally, thereby reducing hardware and management costs. (3) Users do not need to participate in daily maintenance work, just focus on enjoying the service. (4) Location independence; that is, users are not restricted by location. However, cloud storage has a fatal flaw-security [16,22,23]. In recent years, cloud security incidents have occurred frequently. In 2018, some Alexa deployed on AWS began to experience loss of sound. The fault indicator of the smart speaker kept flashing to indicate service interruption. In 2021, the private cloud server of Kronos, a cloud human resources management company, was compromised, resulting in the theft of sensitive customer information. In 2022, Microsoft's public cloud server caused a data breach due to a power outage configuration error. And incidents like this type of case continue to occur. Thus, how to ensure the security of cloud storage is a problem that must be considered. In addition, when users upload data to the Cloud Service Provider (CSP), the data integrity on the cloud is transparent because they no longer have physical control over the data. The security of data storage should not be at the expense of any losses [13,14]. Therefore, guaranteeing the security and integrity of the cloud data simultaneously is an issue worth pondering [4,15].

Currently, biometric feature data, including fingerprints, faces, iris, palm prints, voice prints, etc., have been widely applied in security verification. For example, face unlocking and fingerprint unlocking of smart phones; iris unlocking of bank vaults, etc. Biometrics are human features that make up an individual's identity, such as facial features, iris, and even heartbeat. It has these characteristics [31,33]: (1) Universality refers to that everyone has it. (2) Uniqueness means that the biological characteristics of the same person are unique and generally do not change. (3) Collectability. With the aid of the specialized equipment can be convenient and fast collection. (4) Stability. When as a password, it will not be forgotten or cracked like the normal password. The above features enable it to be used to access scenes such as government and commercial offices, industrial automation systems, personal laptops, and mobile phones. Despite its many advantages, it also causes security issues in the era of massive information. How to use biometric

data to maximize strengths and avoid weaknesses has become a research hotspot. Its popularity has attracted the attention of scholars who study security issues. And this paper focuses on applying biometric feature data to solve the problem of data integrity.

1.1 Related Work

To verify the integrity of remote data, Ateniese *et al.* proposed the Provable Data Possession (PDP) scheme [2]. The PDP scheme is the first scheme to propose random sampling of data on the CSP end. Thus, it is an effective probabilistic checking model. The PDP scheme saves I/O overhead to a great extent while achieving blockless verification. On the other hand, Juels *et al.* proposed another data integrity verification scheme- Proof of Retrievability (PoR) [18] which is implemented in bilinear pairing. This scheme can not only verify the integrity of remote data, but also retrieve data. Unfortunately, neither the PDP nor the PoR scheme mentions the dynamic operation of data blocks. Subsequently, more data integrity schemes that can realize dynamic operations are proposed. Based on symmetric key cryptography, Ateniese *et al.* [3] provided a scalable PDP scheme which can achieve modification, deletion and append operations. Manipulating authenticated dictionaries based on rank information, Erway *et al.* [7] raised a dynamic PDP scheme. Goyal *et al.* [9] put forward a key-policy attribute-based encryption for fine-grained sharing of encrypted data. In addition, more novel data integrity verification schemes were designed in different application scenes. Li *et al.* [20] discussed the generation and storage of duplicate files in a multi-cloud environment, as well as the way of integrity verification. Zhang *et al.* [38] used blockchain as a data storage tool, effectively ensuring that sensitive data cannot be forged, and content can be traced. Fu *et al.* [8] focused on the privacy protection of the shared data holders in the group and constructed a homomorphic verifiable group signature.

There are three modes of remote data integrity checking: private verification, public verification, and delegate verification [34]. Among them, assisting by the Third-Party Auditor (TPA), public auditing has become a popular pattern in the public cloud storage environments. Under the user's authorization, the TPA replaces the user to perform data integrity verification work. Based on PoR, Shacham *et al.* [28] proposed two schemes which can complete the public verifiability and private verifiability using BLS signature and pseudorandom function respectively. Guo *et al.* [11] considered the problem that the dishonest auditors may be performing wrong work. After group users perform dynamic operations (such as: delete, insert) to update data, it will bring huge storage cost for the TPA, so to achieve full dynamic operation, He *et al.* [12] proposed a dynamic group-oriented PDP scheme. Zhao *et al.* [39] focused on practicability and designed a scheme that can realize data dynamics and audit privacy protection at the same time. Gudeme *et al.* [10] proposed a shared data integrity checking scheme, which is constructed on attribute-based encryption and can ensure the efficiency of group user revocation. Yang *et al.* [36] considered the situation of cloud servers dishonestly deleting outsourced data and designed a scheme utilizing Merkle Hash Tree to verify the correctness of audit proof. Nayak *et al.* [25] proposed a public auditing scheme that supports multiple functions, such as: data block dynamics, batch auditing, and privacy protection. Shu *et al.* [30] proposed a decentralized public audit scheme using the Ethereum blockchain, which can effectively prevent the TPA from colluding with malicious absenteeism on the blockchain, resulting in deviation of audit results.

In the development of modern cryptography, Public Key Infrastructure (PKI) has played an important role. It is widely deployed in public key-based security schemes and distributes private keys to users. But to be exact, it has some limitations [6]. On the one hand, in the public key cryptography scheme that uses the PKI to distribute keys, the efficiency is low due to the existence of certificates. On the other hand, the private key dispensed by the PKI must be transmitted through a secure channel and needs to be kept by the user in a highly confidential manner. Once the interaction error occurs, or the private key is lost, it will cause serious losses to the user. Intuitively, it is extremely inconvenient and unsafe. Using Identity- Based Encryption (IBE) to obtain the user's private key can solve the problems caused by the PKI, and user have without access to the public key certificate. IBE uses the user's public identity as the public key and gains the corresponding private key. The advantages have: (1) There is no need for the existence of the PKI. (2) The recipient does not need to be online at any time, just disclose his/her identity that can be used as a public key. But in fact, in the traditional IBE scheme, to acquire the matched private key, the user must request the assistance of the Private Key Generator (PKG). There exists a problem: Only when the valid identity and the user form a perfect correspondence, the PKG will hand out the private key to the user, which inevitably involves supplementary documents or credentials.

One promising approach is to use biometric data as the cryptographic private key. And to be precise, it also belongs to the research category of IBE. But it is unique, this prominent advantage allows the user does not need to worry about the loss of the private key. Unfortunately, the characteristics of noise and fluctuations determine that the biometric data cannot be directly used as a cryptographic key. How to convert biometric data into available information is a critical task. Considering this problem, Doies *et al.* [5] created an efficient secure technique that turns noisy information into a usable key that can be utilized in any cryptographic application. However, due to the existence of the fuzzy extractor, some auxiliary data called a helper string is inevitably. To solve this, Takahashi *et al.* [32] provided a fuzzy signature scheme. In reference [32], assisting by fuzzy key setting to change fuzzy data into available feature vectors, a novel definition of

signing a message called Fuzzy Signature is given, and the signature is verified by linear sketch. Subsequently, based on previous work, Matsuda *et al.* [24] put forward an improved fuzzy signature scheme. Under public cloud storage, with biometric data as the private key, some scholars who concentrate on the data integrity checking scheme have conducted some profound studies. To realize the private key no need to store, Shen *et al.* [29] gave a public auditing scheme that can support blockless verification and fuzzy identity signature. Kaga *et al.* [19] applied biometric data into the blockchain and proposed a signature scheme which was implemented in an IoT blockchain system. Integrating biometric data with cryptography techniques, Abbdal *et al.* [1] presented a scheme which based on XOR operation and iris feature extraction. Based on fuzzy identity- based encryption [27], Li *et al.* [21] formalized a new primitive of fuzzy identity-based data auditing, in which the user identity is a set of descriptive attributes instead of a specific one. Besides, more multi-scenario schemes using biometric data as private keys have been presented [17, 26, 37, 40].

1.2 Contributions

Using biometric data as the encrypted private key for data integrity verification is a hot topic, but the file's tag is directly related to the number of the feature vectors in most existing schemes. Thus, in our proposal, we turn biometric data into user's private key, and the contributions are summarized as follows:

- To convert biometric data into user's private key, we propose a new method named fuzzy identity processing (FIP) executed by the user. In FIP, the feature vectors extracted from user's biometric data will compose a vector space. FIP selects some random vectors, gathers them into an aggregate vector, and performs a series of processing on it to make it as the user's identity. The valid identity in our scheme is generated by the user rather than the PKG, which avoids the usage of supplementary documents or credentials.
- In the tag generation phase, the valid identity will help user generate private key, and further calculate the tags set of outsourced files. Emphasizing that the tag design of our proposed scheme is independence with the number of feature vectors, which can greatly reduce the computational overhead and storage space. In the auditing phase, when a user possess a feature vector wants to view the audit result, the TPA only needs to judge whether the feature vector comes from the vector space. The existence of vector space can help authorized users to quickly get TPA's certification.
- With the given query-forgery model, the soundness of our scheme based on the Computational Diffie-Hellman (CDH) assumption and the Discrete Logarithm (DL) assumption have been rigorously proven. Besides, the performance evaluation demonstrates that the scheme is effective and feasibility.

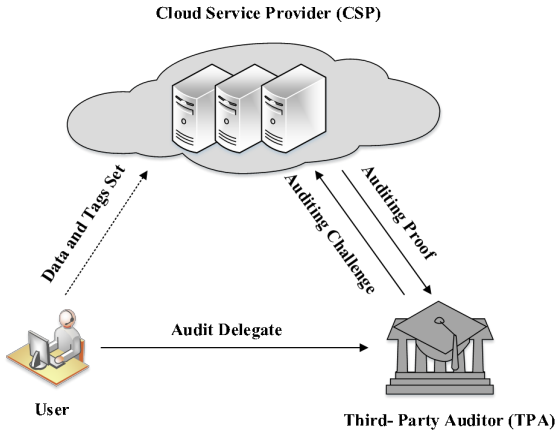


Figure 1: The system model diagram

2 Preliminaries

In this section, we describe the system model, design goals, and cryptographic knowledge.

2.1 System Model

The system model is shown in Figure 1. The system consists of three entities:

1) Users: the users of the public cloud storage services, possess outsourced data that need to be uploaded to the CSP.

2) Cloud Service Provider (CSP): the untrusted entity that provides public cloud storage service.

3) Third-Party Auditor (TPA): the trusted entity who is delegated by the user to perform remote data integrity checking.

2.2 Design Goals

A Public data integrity auditing scheme based on fuzzy identity should achieve following goals:

1) Audit Correctness: If the CSP completely stores the user's cloud data, the proof generated by the CSP can be verified by the TPA.

2) Audit Soundness: If the CSP does not possess user's intact data, the audit proof it provides will fail the TPA's correctness verification.

2.3 Cryptographic Knowledge

Bilinear Map. Let G_1, G_2 are multiplicative cyclic group with the order p, g is a generator of G_1. A bilinear map $e : G_1 \times G_1 \longrightarrow G_2$ satisfies the following properties:

1) Bilinearity: $\forall u, v \in G_1$ and $\forall a, b \in Z_P^*$, $e(u^a, v^b) = e(u, v)^{ab}$;
2) Non-degeneracy:$e(g_1, g_2) \neq 1$;
3) Computable: there is an efficient algorithm to calculate e.

Computational Diffie- Hellman Assumption. For unknown $\forall a, b \in Z_P^*$, given g, g^a and g^b as input, output $g^{ab} \in G_1$.

Definition 1. *(CDH assumption). The advantage of a PPT (probabilistic polynomial time) algorithm $\mathcal{A}$ in solving the CDH problem in G_1 defined below is negligible:*

$$AdvCDH_{\mathcal{A}} = \Pr\left[\mathcal{A}\left(g, g^a, g^b\right) = g^{ab} : a, b \overset{R}{\leftarrow} Z_P^*\right]$$

Discrete Logarithm Assumption. For unknown $\forall x \in Z_P^*$, given g and g^x as input, output x.

Definition 2. *(DL assumption). The advantage of a PPT (probabilistic polynomial time) algorithm $\mathcal{A}$ in solving the DL problem in G_1 defined below is negligible:*

$$AdvDL_{\mathcal{A}} = \Pr\left[\mathcal{A}\left(g, g^x\right) = x : x \overset{R}{\leftarrow} Z_P^*\right]$$

3 Overview of the Proposed Scheme

3.1 System Components

A public data integrity auditing scheme based on fuzzy identity consists of six algorithms: **Setup**, **KeyGen**, **TagGen**, **Challenge**, **ProofGen**, **ProofVerify**. Each algorithm is described as follows:

Setup is the "setup" algorithm that takes the security parameter k as input, and outputs the system public parameter pp.

KeyGen is the "private key generation" algorithm that takes the system public parameter pp and user identity K_m as input, and outputs user's private key SK_{ID}.

TagGen is the "tag generation" algorithm that takes user's private key SK_{ID} and encrypted file F as input, and outputs the tags set T. Then, the user uploads $\langle F, T\rangle$ to the CSP.

Challenge algorithm that generates the integrity challenge $chal$.

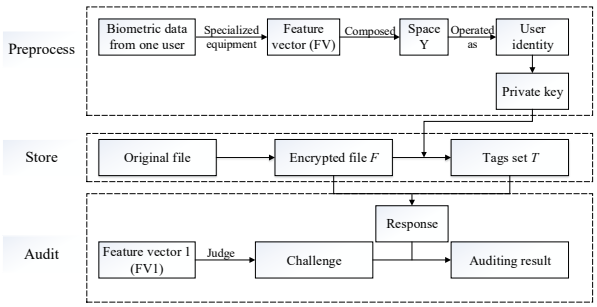


Figure 2: The system basic architecture diagram

ProofGen is the "proof generation" algorithm that takes the integrity challenge $chal$, user's encrypted file F and tags set T as input, and outputs the audit proof F.

ProofVerify is the "proof verification" algorithm that takes system public parameter pp, integrity challenge $chal$ and the audit proof P as input, and outputs "0/1"; "1" indicates that the data stored on the CSP is intact; otherwise, it is not.

3.2 Basic Idea

A public data integrity auditing scheme based on fuzzy identity consist of three procedures, namely: Preprocess, Store and Audit. Figure 2 shows more details.

Preprocess: Which includes **Setup** and **KeyGen** algorithms. The responsibility is to process the biometric data through a series of operations and convert it into an available identity for the user. When biometric data, such as iris, fingerprint, are extracted from the user, they will be processed into feature vector (FV) with the help of the specialized equipment. Space **Y** is composed by feature vectors from one user. Different from other schemes (they use all feature vectors or one feature vector to generate user's private key, like reference [21, 27]), our scheme chooses some feature vectors from the space **Y** assisting by given criteria. The selected feature vectors can be directly used as the user's available identity via calculations. Then, the private key can be obtained.

Store: Which consists of **TagGen** algorithm. In this procedure, the user encrypts the file and generates the tags set.

Audit: Which includes **Challenge**, **ProofGen** and **ProofVerify** algorithms. In this stage, the TPA performs public auditing for the user. Mentioning that all valid vectors from the user's space **Y** can be recognized as a usable vector. That is, if someone is authorized by the user and obtains a usable vector, he/she can notify the TPA to execute audit and view the result.

4 Fuzzy Identity Processing

In this section, after acquiring the feature vector from the user's biometric data, we provide a new method named fuzzy identity processing (FIP) to get the user's available identity. With the help of FIP, the user can get an available identity and further calculate the private key.

After getting the feature vectors through specialized equipment from the biometric data, it needs to execute operations to obtain a useful identity. Here we first give the definition of the vector space, which is similar with the metric space given in reference [32].

Definition 3. *Let* $\mathbf{Y}$ *is a vector space, where* $\mathbf{Y} := [0,1\}^m \in R^m$, R *represents the set of all real number, and satisfies* $\mathbf{Y} \times \mathbf{Y} \longrightarrow R^m$. *A vector space consists of the following:*

- $(d, \mathbf{Y})$: $\mathbf{Y}$ *is a vector space. The distance function is* $\hat{d}(\mathbf{y}_i - \mathbf{y}_j) = |\mathbf{y}_i - \mathbf{y}_j|_{1\le i,j\le m, i\neq j}$. *Define the maximum distance* $\hat{d}_{max} = \lfloor max_{1\le i,j\le m, i\neq j} |\mathbf{y}_i - \mathbf{y}_j| \rfloor$ *and the minimum distance* $\hat{d}_{\min} = \lceil \min_{1\le i,j\le m, i\neq j} |\mathbf{y}_i - \mathbf{y}_j| \rceil$.
- Ω: *the uniform distribution of biometric data over* $\mathbf{Y}$.
- ε: *the threshold value*($\varepsilon \in R$). *Two different vectors* $\mathbf{y}_1, \mathbf{y}_2$ *satisfy* $\hat{d}(\mathbf{y}_1, \mathbf{y}_2) < \varepsilon$, *which means that they may come from one vector space.*

For vector $\mathbf{y}_1 = (y_{11}, ..., y_{1m})$ and $\mathbf{y}_2 = (y_{21}, ..., y_{2m})$, Define the notation $< \mathbf{y}_1, \mathbf{y}_2 > \stackrel{\text{def}}{=} \sum_{j=1}^{m} y_{1j} y_{2j}$ denotes the inner product of the two vector $\mathbf{y}_1$ and $\mathbf{y}_2$ (which is similar with the dot product given in reference [35]).

We implement in bilinear map to generate the user's available identity, and the process is given as follows:

Init (1^k)**.**

This is "**Init**" algorithm to initializing public parameters $pp = (G_1, G_2, p, e, g)$, pseudo-random function (PRF): $Z_P^* \times \{1, 2, ..., n\} \to Z_P^*$ and pseudo-random permutation (PRP): $Z_P^* \times \{1, 2, ..., n\} \to \{1, 2, ..., n\}$ (parameters and functions mentioned above are the same as those initialized in the "setup" phase in section 5).

VeGen (pp,**Y**)**.**

This is "vector generation" algorithm that takes the feature vectors as input, and outputs an aggregated vector agg_{vec}.

1) The user determines a PRP key s_0 to generate the index set Q_{ind} from the space $\mathbf{Y}$, where $Q_{ind} = PRP_{s_0}(t)_{1\le t\le s}$.
2) The user selects the corresponding index according to the Q_{ind} and calculates the pre-aggregated vector $agg_{vec}^{'}$, where $agg_{vec}^{'} = \sum_{(i,j)\in Q_{ind}, i\neq j} < \mathbf{y}_i, \mathbf{y}_j > = \sum_{(i,j)\in Q_{ind}, i\neq j} \mathbf{y}_i \mathbf{y}_j = (y_1^{'}, ..., y_m^{'})$.
3) Let $C : R^m \to Z^m$ (Z is the set of all integers) be an integer transformation function which can change the real number into integer. The user computes the aggregated vector $agg_{vec} = agg_{vec}^{'} + C = (\lfloor y_1^{'} + 0.5 \rfloor, ..., \lfloor y_m^{'} + 0.5 \rfloor) = (y_1, ..., y_m)$.

IDGen (agg_{vec}, pp)**.**

The user chooses $(\omega_1, ..., \omega_m) \in Z_P^*$ randomly; Then, the user gains a useful identity K_m through calculating $K_m = \sum_{l=1}^{m} \omega_l y_l + PRF_{s_1}(m) mod p$, where s_1 is the *key* of PRF.

5 The Proposed Scheme

A public data integrity auditing scheme based on fuzzy identity are introduced in detail in this section.

Setup (1^k)

1) The user chooses two multiplicative cyclic groups G_1 and G_2 with prime order p, and g is a generator of G_1. The user selects cryptographic hash function $H : \{0,1\}^* \longrightarrow Z_P^*, H_1, H_2 : \{0,1\}^* \longrightarrow G_1$, the bilinear map $e : G_1 \times G_1 \longrightarrow G_2$, pseudo-random function (PRF) $f : Z_P^* \times \{1, 2, ..., n\} \to Z_P^*$, pseudo-random permutation (PRP) $\pi : Z_P^* \times \{1, 2, ..., n\} \to \{1, 2, ..., n\}$.
2) The user chooses an element $u \in G_1$ at random.
3) The user picks an element $x \in Z_P^*$, computes the master secret key $msk = x$ and master public key $mpk = g^x$.
4) The user publishes the system public parameter $p = (G_1, G_2, p, e, f, \pi, H, H_1, H_2, u, mpk)$ and keeps the master secret key $msk = x$ not shared.

KeyGen (pp, K_m)

The user takes his/her valid identity K_m and public parameter pp as input and computes the private key. The private key is $SK_{ID} = g^x \cdot H_1(K_m)^{\tau}$, where $\tau = H(K_m)$ (The specific process has been given in Section 4).

TagGen (F, SK_{ID})

1) Before creating the tags set, the user encrypts the sourced file is $F^{'}$ as $F = E_{key}(F^{'})$, where *key* is a secret key; then he/she divides F into n blocks $F = \{b_i\}_{1\le i\le n}$.
2) The user sets the $\delta = H_2(name||n||\tau)$, where $name \in Z_P^*$ is a random value selected as the file identifier.
3) The user picks a random element $r \in Z_P^*$ and computes g^r.
4) For block b_i, the user computes $\sigma_i = g^x \cdot H_1(K_m)^{\tau} \cdot (\delta \cdot u^{b_i})^r$, and $T = \{\sigma_i\}_{1\le i\le n}$.

5) The user sends $\langle F, T\rangle$ to the CSP and deletes the local storage.

Challenge

During the public auditing phase, the TPA sends an integrity challenge *chal* to the CSP. The detailed process is as follows:

1) The TPA determines a c, where $1 \le c \le n$.
2) The TPA generates a PRP key k_1 and a PRF key k_2, where $k_1, k_2 \in Z_P^*$.
3) The TPA sends $chal = \{c, k_1, k_2\}$ to the CSP.

ProofGen (*chal*, F, T)

After receiving the *chal*, the CSP generates the audit proof and returns to the TPA. The detailed process is as follows:

1) The CSP computes $\{i\} = \pi_{k_1}(l)_{1\le c\le n}$, $\{v_i\} = f_{k_2}(l)_{1\le c\le n}$.
2) The CSP calculates $\lambda = \sum_{(i,v_i)\in Q} v_i b_i$, $\sigma = \prod_{(i,v_i)\in Q} \sigma_i^{v_i}$.
3) The CSP returns the audit proof $P = \{\lambda, \sigma\}$ to the TPA.

ProofVerify (*pp*, *chal*, P)

The TPA checks the correctness of the proof as follows:

$$\begin{aligned} e(\sigma, g) \stackrel{?}{=} & e(mpk, g)^{\sum_{(i,v_i)\in Q} v_i} \\ & \cdot e\left(H_1\left(K_m\right)^{\tau}, g\right)^{\sum_{(i,v_i)\in Q} v_i} \\ & \cdot e\left(\prod_{(i,v_i)\in Q} \delta^{v_i} \cdot u^{\lambda}, g^{r}\right) \end{aligned} \quad (1)$$

If Equation (1) holds, returns "1", which means that the challenged data stored in the CSP is intact; Otherwise, returns "0".

6 Security Analysis

In this section, we prove that the proposed scheme is secure in term of the audit correctness and audit soundness.

Theorem 1. *(Audit Correctness) If the CSP completely stores the user's data, the audit proof generated by the CSP can be verified by the TPA.*

Proof. In **ProofVerify** algorithm, the TPA verify the correctness by checking what Equation (1) holds.

$$\begin{aligned} e(\sigma, g) &= e\left(\prod_{(i,v_i)\in Q} \sigma_i^{v_i}, g\right) \\ &= e\left(\prod_{(i,v_i)\in Q} \left(g^x \cdot H_1\left(K_m\right)^{\tau} \cdot \left(\delta \cdot u^{b_i}\right)^{r}\right)^{v_i}, g\right) \\ &= e\left(\prod_{(i,v_i)\in Q} \left(g^x\right)^{v_i}, g\right) \cdot e\left(\prod_{(i,v_i)\in Q} \left(H_1\left(K_m\right)^{\tau}\right)^{v_i}, g\right) \\ &\quad \cdot e\left(\prod_{(i,v_i)\in Q} \left(\left(\delta \cdot u^{b_i}\right)^{r}\right)^{v_i}, g\right) \\ &= e\left(\left(g^x\right)^{\sum_{(i,v_i)\in Q} v_i}, g\right) \cdot e\left(\left(H_1\left(K_m\right)^{\tau}\right)^{\sum_{(i,v_i)\in Q} v_i}, g\right) \\ &\quad \cdot e\left(\prod_{(i,v_i)\in Q} \delta^{v_i} \cdot \prod_{(i,v_i)\in Q} u^{b_i v_i}, g^{r}\right) \\ &= e\left(g^x, g\right)^{\sum_{(i,v_i)\in Q} v_i} \cdot e\left(H_1\left(K_m\right)^{\tau}, g\right)^{\sum_{(i,v_i)\in Q} v_i} \\ &\quad \cdot e\left(\prod_{(i,v_i)\in Q} \delta^{v_i} \cdot u^{\sum_{(i,v_i)\in Q} b_i v_i}, g^{r}\right) \\ &= e(mpk, g)^{\sum_{(i,v_i)\in Q} v_i} \cdot e\left(H_1\left(K_m\right)^{\tau}, g\right)^{\sum_{(i,v_i)\in Q} v_i} \\ &\quad \cdot e\left(\prod_{(i,v_i)\in Q} \delta^{v_i} \cdot u^{\lambda}, g^{r}\right) \end{aligned}$$

If Equation (1) holds, it indicates that the challenged data stored in the CSP is intact, returns "1"; Otherwise, returns "0". □

Theorem 2. *(Audit Soundness) If the CDH assumption and DL assumption hold in G_1, and the tags set is existentially unforgeable; then, the CSP cannot pass TPA's correctness verification with negligible probability, in the case that it does not fully possess user's intact file.*

Proof. We use the query-forgery model to prove the security of the scheme. Assume that the CSP acts as an adversary $\mathcal{A}$, and the TPA is regarded as the challenger $\mathcal{C}$, which is similar to reference [28]. By executing the following series of games to implement multiple interactions between $\mathcal{A}$ and $\mathcal{C}$, the soundness of the proposed scheme can be proved.

Game 0: The adversary $\mathcal{A}$ asks the challenger $\mathcal{C}$ to obtain the system public parameter *pp*, then the challenger $\mathcal{C}$ runs the **Setup** algorithm and returns *pp*. Then, the adversary $\mathcal{A}$ makes two types of queries: (1) The adversary $\mathcal{A}$ queries the user's private key SK_{ID}, then the challenger $\mathcal{C}$ returns SK_{ID} by running the **KeyGen** algorithm. (2) The adversary $\mathcal{A}$ queries the tags set T of the encrypted file F, then the challenger $\mathcal{C}$ returns T by running the **TagGen** algorithm. Further, the challenger $\mathcal{C}$ sends the integrity challenge *chal* and asks the adversary $\mathcal{A}$ to

provide the audit proof P. Upon received, the adversary $\mathcal{A}$ computes and replies to the challenger $\mathcal{C}$. Once the audit proof P that is successfully checked by the challenger $\mathcal{C}$ with non-negligible probability, we say that the adversary $\mathcal{A}$ has won the game.

Game 1: Game 1 is the same as **Game 0**, but there exist a minor difference. The challenger $\mathcal{C}$ keeps a list with recording all tags that the adversary $\mathcal{A}$ has ever queried. Whenever the adversary $\mathcal{A}$ makes the **TagGen** query, the challenger $\mathcal{C}$ adds a record to this list.

Game 2: Game 2 is the same as **Game 1**, but there exist a minor difference. The challenger $\mathcal{C}$ keeps a list with recording all responses that the adversary $\mathcal{A}$ has ever respond.

If the response $P = \{\lambda, \sigma\}$ returned by the CSP can be pass the TPA's verification, the proof P must correct; That is, given a valid audit proof $P = \{\lambda, \sigma\}$, it can successfully pass the verification of the following equation.

$$\begin{aligned} e(\sigma, g) &= e(mpk, g)^{\sum_{(i,v_i)\in Q} v_i} \\ &\quad \cdot e\left(H_1\left(K_m\right)^{\tau}, g\right)^{\sum_{(i,v_i)\in Q} v_i} \\ &\quad \cdot e\left(\prod_{(i,v_i)\in Q} \delta^{v_i} \cdot u^{\lambda}, g^{r}\right) \end{aligned} \quad (2)$$

Assume that there exist a response $P^{'}$ forged by the adversary $\mathcal{A}$ have passed challenger $\mathcal{C}$'s correctness verification by checking Equation (2), we say that the adversary $\mathcal{A}$ won the game. But the aggregated signature $\sigma^{'} = \prod_{(i,v_i)\in Q} \sigma_i^{'v_i}$ is not equal to σ, then the challenger $\mathcal{C}$ aborts this game even if the adversary $\mathcal{A}$ has won the game.

Analysis: Assume that the adversary $\mathcal{A}$ wins the **Game 2** with non-negligible probability. Then, we construct a simulator to solve the CDH problem. The goal of the simulator is to output h^{α} when g, g^{α}, h as input. The simulator acts like the challenger $\mathcal{C}$ in **Game 1**, but has some difference:

1) It randomly selects an element $x \in Z_P^*$, and sets the master secret key $msk = x$, the master public key $mpk = g^x$. Then, it chooses two random values $a, b \in Z_P^*$ and sets $u = g^a h^b$.
2) It generates the private key $SK_{ID} = g^x \cdot H_1(K_m)^{\tau}$.
3) It continue interacts with the adversary $\mathcal{A}$. Upon received the forged proof $P^{'}$ from the adversary $\mathcal{A}$, the simulator checks whether Equation (3) is true:

$$\begin{aligned} e(\sigma^{'}, g) &= e(mpk, g)^{\sum_{(i,v_i)\in Q} v_i} \\ &\quad \cdot e\left(H_1\left(K_m\right)^{\tau}, g\right)^{\sum_{(i,v_i)\in Q} v_i} \\ &\quad \cdot e\left(\prod_{(i,v_i)\in Q} \delta^{v_i} \cdot u^{\lambda^{'}}, g^{r}\right) \end{aligned} \quad (3)$$

If the adversary $\mathcal{A}$ can pass the verification, it means that the adversary $\mathcal{A}$ won; but the tag $\sigma \neq \sigma^{'}$, then this game aborts.

Obviously, $\lambda \neq \lambda^{'}$; otherwise, $\sigma \neq \sigma^{'}$, which contradicts our assumption. We define $\triangle\lambda = \lambda^{'} - \lambda$. Now, we dividing Equation (3) by Equation (2) and assuming $g^r = (g^{\alpha})^{\bar{x}}$, we have:

$$e\left(\sigma'/\sigma, g\right) = e\left(u^{\Delta\lambda}, g^{r}\right) = e\left(\left(g^a h^b\right)^{\Delta\lambda}, \left(g^{\alpha}\right)^{\bar{x}}\right)$$

Then, we can obtain

$$\begin{aligned} e\left(\sigma' \cdot \sigma^{-1} \cdot \left(g^{\alpha}\right)^{-\Delta\lambda\bar{x}a}, g\right) &= e\left(h^{\alpha}, g\right)^{\Delta\lambda\bar{x}b} \\ &= e\left(h^{\alpha}, g\right)^{\Delta\lambda\bar{x}b} \end{aligned}$$

Further we can get $\left(\sigma' \cdot \sigma^{-1} \cdot \left(g^{\alpha}\right)^{-\Delta\lambda\bar{x}a}\right)^{1/\Delta\lambda\bar{x}b} = h^{\alpha}$. Clearly that the probability of game failure is equivalent to calculate the probability of $\Delta\lambda\bar{x}b = 0 mod p$. The probability of $\Delta\lambda\bar{x}b = 0 mod p$ is $1/p$ which is negligible since p is a large prime. Hence, we can solve the CDH problem with a probability $1-1/p$, which contradicts assumption that CDH problem in G_1 is computationally infeasible.

Game 3: Game 3 is the same as **Game 2**, but there exist a minor difference. The challenger $\mathcal{C}$ also keeps a list with recording all responses that the adversary $\mathcal{A}$ has ever respond. If the the adversary $\mathcal{A}$ have passed challenger $\mathcal{C}$'s verification, but the aggregate message $\lambda^{'}$ is not equal to λ, then the challenger $\mathcal{C}$ aborts this game even if the adversary $\mathcal{A}$ has won the game.

Analysis: Assume that the adversary $\mathcal{A}$ wins the **Game 3** with non-negligible probability. Then, we construct a simulator to solve the DL problem. The goal of the simulator is to output α when $g, h = g^{\alpha}$ as input. The simulator acts like the challenger $\mathcal{C}$ in **Game 2**, and the process is same as the **Game 2**, but has some difference.

It also chooses two random values $a, b \in Z_P^*$ and sets $u = g^a h^b$. If the adversary $\mathcal{A}$ can pass verification, Equation (3) will be true, and it means that the adversary $\mathcal{A}$ won; but $\lambda \neq \lambda^{'}$, then this game aborts. Here we know $\sigma \neq \sigma^{'}$ but $\lambda \neq \lambda^{'}$. Define $\triangle\lambda = \lambda^{'} - \lambda$ and dividing Equation (3) by Equation (2), it can obtain:

$$1 = u^{\Delta\lambda} = \left(g^a h^b\right)^{\Delta\lambda} = g^{\Delta\lambda a} \cdot h^{\Delta\lambda b}$$

Clearly that $\triangle\lambda \neq 0 modp$; otherwise, $\lambda^{'} = \lambda modp$, which contradicts aforementioned assumption.

Further, we have $h = g^{-\Delta\lambda a/-\Delta\lambda b} = g^{a/b}$. Obviously that the probability of game failure is equivalent to calculate the probability of $b = 0$. The probability of this is $1/p$ which is negligible since p is a large prime. Hence, we can solve the DL problem with a probability $1 - 1/p$, which contradicts assumption that DL problem in G_1 is computationally infeasible.

From the above games, we know that solving the CDH problem and DL problem in G_1 is computationally infeasible. Further, It implies that the CSP cannot pass the TPA's correctness checking with negligible probability, in the case that it does not fully possess user's intact file.

□

7 Performance Evaluation

7.1 Performance Analysis

Firstly, we evaluate the performance of the proposed scheme in terms of computation overhead. For simplicity, we give the meaning of the following notations. Here c indicates the number of the challenged blocks. H_{G_1} denotes the hash operation in G_1. Exp_{G_1}, Exp_{G_2} and $Exp_{Z_P^*}$ respectively express the exponentiation operation in G_1, G_2 and Z_P^*. Mul_{G_1}, Mul_{G_2} and $Mul_{Z_P^*}$ mean the multiplication operation in G_1, G_2 and Z_P^* respectively. $Pair$ represents the pairing operation in multiplicative cyclic group. $Add_{Z_P^*}$ indicates the addition operation in Z_P^*. C_f means the PRF or PRP operation.

We compare scheme [28] and [29] in term of computation overhead on the server side and TPA side as shown in Table 1. Regarding the **ProofGen** algorithm, scheme [28] and [29] have the same computational overhead. Compared with them, our scheme requires an extra PRF and PRP operations, where PRP operation is to generate the index of the challenged blocks and PRF operation is to create a random number set.

As for the **ProofVerify** algorithm, in scheme [29], due to the verification key vk needs to be checked, it is necessary to perform more $Exp_{Z_P^*} + P + C$ operations on the TPA side, P and C denote two important operations in scheme [29]. Compared with scheme [28], for computing $\sum_{(i,v_i)} v_i$ once, our scheme requires to perform $(c-1)$ addition operations in Z_P^*. And calculating the computation cost of the $\prod_{(i,v_i)\in Q} \delta^{v_i}$ is $H_{G_1} + cExp_{G_1} + (c-1)Mul_{G_1}$. In addition, to verify the right side of Equation (1), our scheme needs to carry out two exponentiation operations and three pairing operations in G_2.

7.2 Implementation

Then we evaluate the performance of the proposed scheme by several experiments. We run a series of experiments on a 1.8 GHZ Intel Core i5 processor and 8GB RAM. All the experiments using the Type A with the free Pairing-Based Cryptography (PBC) Library. In the implementation, we choose the based filed size to be 512 bits, and the size of Z_P^* to be 160 bits, this is, $|p| = 160$ bits.

To evaluate the performance of different algorithm, we set the file size to 20MB which divided into $1,000$ data blocks and the number of the challenged blocks is 460. As we can see from the Table 2, the most time-saving algorithm is key generation which only needs to generate private key. Specially, the computational overhead is independent of the number of file blocks and challenged blocks, and is executed only once during the initialization phase. In addition, the most time-consuming algorithm is tag generation which almost costs 3728.785ms when the data blocks are $1,000$. The overhead of the proof generation algorithm and proof verification algorithm is associated with the number of the challenged blocks. When $c = 460$, it takes about 1791.104ms and 3538.271ms respectively.

In the second part, we evaluate the performance of tag generation algorithm which is most expensive and time consuming. We set the file is 20MB and 200MB respectively and the number of the data blocks from 0 to $1,000$, increased by an interval of 100. Figure 3 reflects the difference. It can be noticed that the tag generation time is directly linked with the file size. Namely, the larger the file, the more time it takes. However, when the files are 20MB and 200MB, the time difference is smaller. From the perspective of tag design, it is apparent that the divergence originates from the size of a single data block. Likewise, the number of data blocks will also affect the computational time. But fortunately, computing tags for one file is a one-time task.

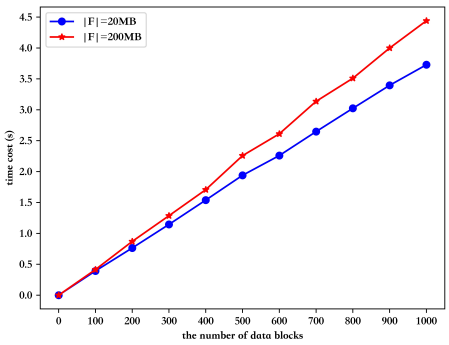


Figure 3: Comparison of the time cost when the file size is different

To evaluate the performance, we compare the time cost of our scheme with scheme [29] in the proof generation and proof verification phases. We set the number of the challenged blocks from 0 to $1,000$, increased by an interval of $1,000$ (Here we also set the file size to 20MB but divided

Table 1: Comparison of computation overhead on the server side and TPA side

Scheme	**Server**	**TPA**
Scheme [12]	$c\,\mathrm{Exp}_{G_1}+(c-1)Mul_{G_1}+cMul_{z_p^*}+(c-1)Add_{z_p^*}$	$2\mathrm{Pair}+(c+1)\,\mathrm{Exp}_{G_1}+cMul_{G_1}+cH_{G_1}$
Scheme [24]	$c\,\mathrm{Exp}_{G_1}+(c-1)Mul_{G_1}+cMul_{z_p^*}+(c-1)Add_{z_p^*}$	$2\mathrm{Pair}+(c+2)\,\mathrm{Exp}_{G_1}+cMul_{G_1}+cH_{G_1}+\mathrm{Exp}_{z_P^*}+P+C$
Our Scheme	$c\,\mathrm{Exp}_{G_1}+(c-1)Mul_{G_1}+cMul_{z_p^*}+(c-1)Add_{z_p^*}+cC_f$	$4\mathrm{Pair}+(c+2)\,\mathrm{Exp}_{G_1}+2\,\mathrm{Exp}_{G_{G_2}}+cMul_{G_1}+2Mul_{G_2}+2(c-1)Add_{z_p^*}+2H_{G_1}+2C_f$

Table 2: Performance of different algorithm

Algorithm	**Key generation**	**Tag generation**	**Proof generation**	**Proof Verification**
time cost (ms)	55.721	3728.785	1791.104	3538.271

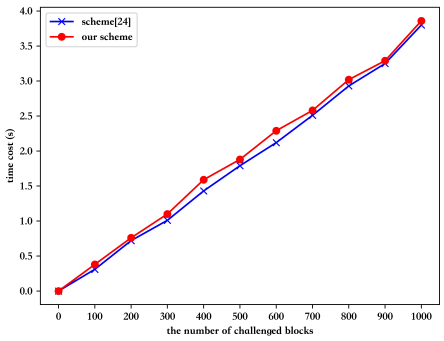


Figure 4: Comparison of the time cost in the proof generation phase between our scheme and scheme [29]

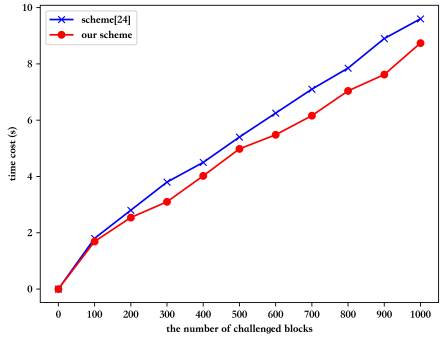


Figure 5: Comparison of the time cost in the proof verification phase between our scheme and scheme [29]

into 1,000,000 data blocks). Figure 4 and Figure 5 give more details. Figure 4 shows the comparison of proof generation algorithm between our scheme and scheme [29]. It clearly observes that our scheme spends slightly longer time than scheme [29], and the reason for this is that our scheme needs to execute PRF operation and PRP operation once. Figure 5 demonstrates that our scheme has slightly lower time consumption than scheme [29] in the proof verification phase. In our scheme, the computation cost of proof generation varies from 0.384s to 3.865s and proof verification varies from 1.697s to 8.749s.

8 Conclusion

This paper propose a public data integrity auditing scheme under public cloud storage environment. In our scheme, we provide a new method named FIP for processing the feature vectors into user's identity to get biometric data as user's private key. A valid identity will be help user generate private key, and further calculate the file tags set. In addition, the tag design is not related to the number of feature vectors, which determines that the computational overhead and storage space can be saved. Besides, with vector space, the TPA can judged quickly whether one feature vector is an authorized vector. Both the security analysis and performance evaluation illustrate the feasibility of the proposed scheme.

Acknowledgments

This work was supported in part by the Scientific Research Common Program of Beijing Municipal Commission of Education (KM202110015004) and the Scientific

Research Common Program of Beijing Municipal Commission of Education (KM202310015002). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] S. Abbdal, H. Jin, D. Zou, and A. Yassin, "Secure and efficient data integrity based on iris features in cloud computing," in *2014 7th International Conference on Security Technology*, pp. 3–6, 2014.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 598–609, 2007.

[3] G. Ateniese, R. Dipietro, L. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in *Proceedings of the 4th international conference on Security and privacy in communication netowrks*, pp. 1–10, 2008.

[4] P. S. Chung, C. W. Liu, and M. S. Hwang, "A study of attribute-based proxy re-encryption scheme in cloud environments", *International Journal of Network Security*, vol. 16, no. 1, pp. 1-13, 2014.

[5] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *International conference on the theory and applications of cryptographic techniques*, pp. 523–540, 2004.

[6] C. Ellison and B. Schneier, "Ten risks of pki: What you're not being told about public key infrastructure," *Computer Security Journal*, vol. 16, no. 1, pp. 1–7, 2000.

[7] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," *ACM Transactions on Information and System Security (TISSEC)*, vol. 17, no. 4, pp. 1–29, 2015.

[8] A. Fu, S. Yu, Y. Zhang, H. Wang, and C. Huang, "Npp: A new privacy-aware public auditing scheme for cloud data sharing with group users," *IEEE Transactions on Big Data*, vol. 8, no. 1, pp. 14–24, 2017.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Water, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM conference on Computer and communications security*, pp. 89–98, 2006.

[10] J. Gudeme, S. Pasupuleti, and R. Kandukuri, "Attribute-based public integrity auditing for shared data with efficient user revocation in cloud storage," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 2019–2032, 2021.

[11] W. Guo, H. Zhang, S. Qin, F. Gao, Z. Jin, W. Li, and Q. Wen, "Outsourced dynamic provable data possession with batch update for secure cloud storage," *Future Generation Computer Systems*, vol. 95, pp. 309–322, 2019.

[12] K. He, J. Chen, Q. Yuan, S. Ji, D. He, and R. Du, "Dynamic group-oriented provable data possession in the cloud," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, pp. 1394–1408, 2019.

[13] W. F. Hsien, C. C. Yang and M. S. Hwang, "A survey of public auditing for secure data storage in cloud computing," *International Journal of Network Security*, vol. 18, no. 1, pp. 133-142, 2016.

[14] M. S. Hwang, C. C. Lee, T. H. Sun, "Data error locations reported by public auditing in cloud storage service," *Automated Software Engineering*, vol. 21, no. 3, pp. 373–390, Sep. 2014.

[15] M. S. Hwang, T. H. Sun, "Using smart card to achieve a single sign-on for multiple cloud services," *IETE Technical Review*, vol. 30, no. 5, pp. 410–416, 2013.

[16] M. S. Hwang, T. H. Sun, C. C. Lee, "Achieving dynamic data guarantee and data confidentiality of public auditing in cloud storage service," *Journal of Circuits, Systems, and Computers*, vol. 26, no. 5, 2017.

[17] C. Jin, Y. Xu, G. Chen, C. Yu, Y. Hin, and J. Shan, "Ebiac: Efficient biometric identity-based access control for wireless body area networks," *Journal of Systems Architecture*, vol. 121, p. 102317, 2021.

[18] A. Juels and B. Kaliski, "Pors: Proofs of retrievability for large files," in *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 584–597, 2007.

[19] Y. Kaga, M. Fujio, K. Naganuma, K. Takahashi, T. Murakami, T. Ohki, and M. Nishigaki, "A secure and practical signature scheme for blockchain based on biometrics," in *Information Security Practice and Experience: 13th International Conference*, pp. 877–891, 2017.

[20] J. Li, H. Yan, and Y. Zhang, "Efficient identity-based provable multi-copy data possession in multi-cloud storage," *IEEE Transactions on Cloud Computing*, vol. 10, no. 1, pp. 356–365, 2019.

[21] Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni, and K. Choo, "Fuzzy identity-based data integrity auditing for reliable cloud storage systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 1, pp. 72–83, 2017.

[22] C. W. Liu, W. F. Hsien, C. C. Yang, M. S. Hwang, "A survey of attribute-based access control with user revocation in cloud data storage", *International Journal of Network Security*, vol. 18, no. 5, pp. 900-916, 2016.

[23] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for shared data storage with user revocation in cloud computing", *International Journal of Network Security*, vol. 18, no. 4, pp. 650–666, 2016.

[24] T. Matsuda, K. Takahashi, T. Murakami, and G. Hanaoka, "Fuzzy signatures: relaxing requirements and a new construction," in *Applied Cryp-*

tography and Network Security: 14th International Conference, pp. 97–116, 2016.

[25] S. Nayak and S. Tripathy, "Sepdp: Secure and efficient privacy preserving provable data possession in cloud storage," *IEEE Transactions on Services Computing*, vol. 14, no. 3, pp. 876–888, 2018.

[26] B. Nivedetha and I. Vennila, "Ffbks: Fuzzy fingerprint biometric key based security schema for wireless sensor networks," *Computer Communications*, vol. 150, pp. 94–102, 2020.

[27] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology–EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 457–473, 2005.

[28] H. Shacham and B. Waters, "Compact proofs of retrievability," *Journal of cryptology*, vol. 26, no. 3, pp. 442–483, 2013.

[29] W. Shen, J. Qin, J. Yu, R. Hao, J. Hu, and J. Ma, "Data integrity auditing without private key storage for secure cloud storage," *IEEE Transactions on Cloud Computing*, vol. 9, no. 4, pp. 1408–1421, 2019.

[30] J. Shu, X. Zou, X. Jia, W. Zhang, and R. Xie, "Blockchain-based decentralized public auditing for cloud storage," *IEEE Transactions on Cloud Computing*, vol. 10, no. 4, pp. 2366–2380, 2021.

[31] D. Sun and Z. Qiu, "A survey of the emerging biometric technology," *ACTA ELECTONICA SINICA*, vol. 29, no. S1, p. 1744, 2001.

[32] K. Takahashi, T. Matsuda, T. Murakami, G. Hanaoka, and M. Nishigaki, "Signature schemes with a fuzzy private key," *International Journal of Information Security*, vol. 18, pp. 581–617, 2019.

[33] J. Unar, W. Seng, and A. Abbasi, "A review of biometric technology along with trends and prospects," *Pattern recognition*, vol. 47, no. 8, pp. 2673–2688, 2014.

[34] H. Wang, D. He, and S. Tang, "Identity-based proxy-oriented data uploading and remote data integrity checking in public cloud," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1165–1176, 2016.

[35] J. Xu, A. Yang, J. Zhou, and D. Wong, "Lightweight delegatable proofs of storage," in *Computer Security–ESORICS 2016: 21st European Symposium on Research in Computer Security*, pp. 324–342, 2016.

[36] C. Yang, X. Tao, and Q. Chen, "New publicly verifiable data deletion supporting efficient tracking for cloud storage," *International Journal of Network Security*, vol. 22, no. 5, pp. 885–896, 2020.

[37] Y. Yu, Y. Li, B. Yang, W. Susilo, G. Yang, and J. Bai, "Attribute-based cloud data integrity auditing for secure outsourced storage," *IEEE Transactions on Emerging Topics in Computing*, vol. 8, no. 2, pp. 377–390, 2017.

[38] G. Zhang, Z. Yang, and W. Liu, "Blockchain-based privacy preserving e-health system for healthcare data in cloud," *Computer Networks*, vol. 203, p. 108586, 2022.

[39] H. Zhao, X. Yao, and X. Zheng, "Privacy-preserving tpa auditing scheme based on skip list for cloud storage," *International Journal of Network Security*, vol. 21, no. 3, pp. 451–461, 2019.

[40] X. Zhu and C. Cao, "Secure online examination with biometric authentication and blockchain-based framework," *Mathematical Problems in Engineering*, vol. 2021, 2021.

Biography

Yilin Yuan biography. Yilin Yuan received the M.S. degree and Ph.D degree from the Henan Normal University and Beijing University of Technology in 2018 and 2022, respectively. She is currently a lecture with the college of Information Engineering, Beijing Institute of Graphic Communication. Her research interests include cloud computing, security cloud security and blockchain.

Yofan Gu biography. Yifan Gu is currently a master's candidate, joint-educated, at South China Agriculture University and National Research Center of Intelligent Equipment for Agriculture, Beijing Academy of Agriculture and Forestry Sciences, since 2020. His current interest in research focuses on spectral super-resolution reconstruction and biosensors.

Zhenzhen Zhang biography. Zhenzhen Zhang received the B.S. degree in Communication Engineering from Zhengzhou University in 2009, and the Ph.D. degree in Circuits and Systems from Beijing Jiaotong University in 2017. After the completion of her Ph.D. program, she has been working as an lecturer in Beijing Institute of Graphic Communication. Her research interests include video forensics, video watermarking, and information hiding.

On the Stability of Linear Complexity of $2p^2$-periodic q-ary Sequences

Ruoqi Song[1], Zhihua Niu[1], Chenhuang Wu[2], and Meixiang Chen[3]
(Corresponding author: Ruoqi SONG)
School of Computer Engineering and Science, Shanghai University[1]
Shanghai 200444, China
Key Laboratory of Applied Mathematics of Fujian Province University, Putian University[2]
Putian, Fujian 351100, China
Fujian Key Laboratory of Financial Information Processing,Putian University[3]
Putian, Fujian 351100, China
Email: 453279719@qq.com
(Received Dec. 5, 2022; Revised and Accepted May 12, 2023; First Online June 11, 2023)

Abstract

In this work, for $2p^2$-periodic q-ary sequences, we investigate the linear complexity, k-error linear complexity, and the number of k-error sequences. Firstly, We conclude that the linear complexity of the sequences falls within a specific range between p^2-p and $2p^2$. Secondly, by arranging the $2p\times p$ matrix form, the $p\times 2p$ matrix form, and $p\times p$ matrix forms for the sequences, we propose an algorithm to determine the k-error linear complexity segmented expression based on the weight of each column in the matrices and provide an example to illustrate how the algorithm works. Finally, we introduce a method to study the number of k-error sequences of the sequence.

Keywords: K-error Linear Complexity; K-error Sequences; Linear Complexity; Q-ary Sequences; Stream Cipher

1 Introduction

Pseudorandom sequences play an important role in cryptography. In particular they serve as the secret key in symmetric cryptography. Therefore, the design of pseudorandom sequences and cryptographic indicators is the critical research direction. The cryptographic indicators of sequences mainly include: balance, correlation, linear complexity, k-error linear complexity, k-error sequences and so on [3]. In this paper, we determine the values of linear complexity of $2p^2$-periodic q-ary sequences, and then propose a new algorithm for computing k-error linear complexity and the number of k-error sequences, so we introduce the concepts of linear complexity, k-error linear complexity and k-error sequence of sequences.

Let $\mathbb{F}_q=\{0,1,2,...,q-1\}$ be the q-ary field. For a T-periodic sequence S over $\mathbb{F}_q$, the linear complexity, denoted by $LC(S)$, is the length of the shortest linear feedback shift register (LFSR) that generates the sequence, i.e., the smallest positive integer L such that $s_{u+L}=c_{L-1}s_{u+L-1}+\cdots+c_1s_{u+1}+c_0s_u$ for $u\geqslant 0$ and constants $c_0\neq 0$, $c_1,\ldots,c_{L-1}\in\mathbb{F}_q$. Let $S(x)=s_0+s_1x+s_2x^2+\cdots+s_{T-1}x^{T-1}\in\mathbb{F}_q[x]$, which is called the generating polynomial of S. Then the linear complexity over $\mathbb{F}_q$ of S can be computed as

$$LC(S)=T-\deg\left(\gcd\left(x^T-1,S(x)\right)\right), \tag{1}$$

which is the degree of the characteristic polynomial, $\frac{x^T-1}{\gcd(x^T-1,S(x))}$, of the sequence, see [2] for details.

For integers $k\geqslant 0$, the k-error linear complexity over $\mathbb{F}_q$ of S, denoted by $LC_k(S)$, is the least linear complexity over $\mathbb{F}_q$ that can be obtained by changing at most k terms of the sequence per period, i.e.,

$$LC_k(S)=\min_{wt(E)\leqslant k} LC(S+E) \tag{2}$$

where E is the error sequence with period T and $wt(E)$ equals the number of nonzero terms of E per period, i.e., the weight of E. Clearly, $LC_0(S)=LC(S)$ and $T\geqslant LC_0(S)\geqslant LC_1(S)\geqslant\cdots\geqslant LC_l(S)=0$, where $l=wt(S)$, see, e.g. [5, 9] for details.

The k-error linear complexity of a T-periodic sequence S is $LC_k(S)$. If the T-periodic sequence E satisfies $LC(S+E)=LC_k(S)$ and $1\leq wt(E)\leq k$, then E is said to be a k-error sequence of S. Denote the total number of k-error sequences of the sequence S as $M_k(S)$, see, e.g. [5, 14] for details.

Linear complexity and k-error linear complexity are important cryptographic properties of sequences, characterizing the predictability of a sequence to measure its suitability for cryptography. The Berlekamp-Massey algorithm (BM algorithm) [8] proposed in the 1960s pointed

out that knowing any consecutive bits twice its linear complexity can effectively recover the entire sequence. Therefore, from the perspective of cryptography, the linear complexity of a sequence should be as large as possible, while randomly changing several bits of the sequence does not cause a significant decrease in the linear complexity of the sequence, so the k-error linear complexity was introduced to represent the stability of the linear complexity of the sequence.

For the linear complexity and the k-error linear complexity of certain periodic sequences, many fast algorithms with higher efficiency than BM algorithm have been proposed, for example, see [4, 6, 12, 13] for the 2^n-periodic sequences, see [9, 15, 20] for the p^n-periodic sequences, see [16, 18, 21] for the $2p^n$-periodic sequences, and see [17] for the $2^n p^m$-periodic sequences.

Recently, Chen, Wu and Niu et al. proposed a new matrix method to compute the k-error linear complexity of binary p^2-periodic sequence, q-ary p^2-periodic sequence and binary $2p^2$-periodic sequence, where the k-error linear complexity of the sequences can be derived by arranging the sequences into matrices and counting the number of occurrences of each column element in the matrices, see [1, 11, 19] for details. This provides a new perspective for studying the k-error linear complexity of periodic sequences.

There are currently two methods for computing the k-error linear complexity of a $2p^2$ periodic sequence. The first is a cost vector-based algorithm such as those proposed by Wei in [18] and Zhou in [21]. However, this algorithm is difficult to compute and requires continuous iteration until we find the correct k-error linear complexity. Furthermore, the algorithms differ in their branching judgments and both have omissions that do not guarantee the correct k-error linear complexity. Niu and Li later proposed an improved version of the algorithm in [10], but it is still only suitable for a certain value of k and requires tedious computations to find the decreasing point of the linear complexity. The second method is a genetic algorithm that can compute an approximate value for the k-error linear complexity. According to experiments conducted by Li in [10], the accuracy of this method is around 85 percent. However, like the first method, it can only compute the linear complexity for a given k-value. By using the matrix method to compute the linear complexity of a sequence, we can study the different linear complexities of the sequence and count the minimum number of bits needed to change in order to reach each form. By statistically counting these numbers, we can obtain the final k-error linear complexity segmented expression, which allows us to directly determine the k-error linear complexity for any k-value.

In this paper, we arrange the q-ary sequence $S = (s_n)_{n=0}^{\infty}$ of period $2p^2$ into four matrix forms, and then discuss the k-error linear complexity of S by examining the column structure of the matrices using four matrix forms:

the first matrix form is a matrix of size $p \times 2p$, defined as

$$\mathfrak{M}_S = \begin{bmatrix} s_0 & s_1 & \cdots & s_p & \cdots & s_{2p-1} \\ s_{2p} & s_{2p+1} & \cdots & s_{3p} & \cdots & s_{4p-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ s_{2(p-1)p} & s_{2p^2-p+1} & \cdots & s_{2p^2-p} & \cdots & s_{2p^2-1} \end{bmatrix} \triangleq [M_0, M_1, \ldots, M_{2p-1}],$$

where $M_i = \begin{bmatrix} s_i \\ s_{i+2p} \\ \vdots \\ s_{i+2(p-1)p} \end{bmatrix}$ is the $(i+1)$ th column of $\mathfrak{M}_S$ for $0 \leqslant i < 2p$;
the second is a matrix of size $2p \times p$, defined as

$$\mathfrak{A}_S = \begin{bmatrix} s_0 & s_1 & \cdots & s_{p-1} \\ s_p & s_{p+1} & \cdots & s_{2p-1} \\ \vdots & \vdots & \vdots & \vdots \\ s_{p^2} & s_{p^2+1} & \cdots & s_{p^2+p-1} \\ \vdots & \vdots & \vdots & \vdots \\ s_{(2p-1)p} & s_{(2p-1)p+1} & \cdots & s_{2p^2-1} \end{bmatrix} \triangleq \begin{bmatrix} \mathfrak{A}^{(1)} \\ \hline \mathfrak{A}^{(2)} \end{bmatrix},$$

where $\mathfrak{A}^{(1)}$ and $\mathfrak{A}^{(2)}$ are both matrices of size $p \times p$, and $\mathfrak{A}^{(1)} \triangleq \left[\mathfrak{A}_0^{(1)}, \mathfrak{A}_1^{(1)}, \ldots, \mathfrak{A}_{p-1}^{(1)}\right]$, $\mathfrak{A}^{(2)} \triangleq \left[\mathfrak{A}_0^{(2)}, \mathfrak{A}_1^{(2)}, \ldots, \mathfrak{A}_{p-1}^{(2)}\right]$, $\mathfrak{A}_i^{(1)} = \begin{bmatrix} s_i \\ s_{i+p} \\ \vdots \\ s_{i+(p-1)p} \end{bmatrix}$ and $\mathfrak{A}_i^{(2)} = \begin{bmatrix} s_{i+p^2} \\ s_{i+(p+1)p} \\ \vdots \\ s_{i+2(p-1)p} \end{bmatrix}$ are the $(i+1)$ th column of $\mathfrak{A}^{(1)}$ and $\mathfrak{A}^{(2)}$ for $0 \leqslant i < p$, respectively;
the third is a matrix of size $p \times p$, defined as

$$\mathfrak{A}^{(3)} = \mathfrak{A}^{(1)} + \mathfrak{A}^{(2)} \triangleq \left[\mathfrak{A}_0^{(3)}, \mathfrak{A}_1^{(3)}, \ldots, \mathfrak{A}_{p-1}^{(3)}\right],$$

where $\mathfrak{A}_i^{(3)}$ is the $(i+1)$ th column of $\mathfrak{A}^{(3)}$, and $\mathfrak{A}_i^{(3)} = \mathfrak{A}_i^{(1)} + \mathfrak{A}_i^{(2)}$ for $0 \leqslant i < p$.
the fourth is also a matrix of size $p \times p$, defined as

$$\mathfrak{A}^{(4)} = \mathfrak{A}^{(1)} - \mathfrak{A}^{(2)} \triangleq \left[\mathfrak{A}_0^{(4)}, \mathfrak{A}_1^{(4)}, \ldots, \mathfrak{A}_{p-1}^{(4)}\right],$$

where $\mathfrak{A}_i^{(4)}$ is the $(i+1)$ th column of $\mathfrak{A}^{(4)}$, and $\mathfrak{A}_i^{(4)} = \mathfrak{A}_i^{(1)} - \mathfrak{A}_i^{(2)}$ for $0 \leqslant i < p$.

The rest of the paper is organized as follows. The values of the linear complexity of the q-ary sequences with period $2p^2$ are analyzed in Section 2. The k-error linear complexity of the q-ary sequences with period $2p^2$ can be efficiently determined by the proposed algorithm in Section 3, and an example is presented to demonstrate the application of the algorithm. An analysis of how to compute the number of error sequences of a sequence by matrices with an example is presented in Section 4. Conclusions are given in Section 5.

In this paper, we will always assume that $S=(s_n)_{n=0}^{\infty}$ is a q-ary sequence with the least period $2p^2$, and its corresponding matrix forms $\mathfrak{M}_S$, $\mathfrak{A}_S$, $\mathfrak{A}^{(3)}$ and $\mathfrak{A}^{(4)}$ are as described in Section 1, and the generating polynomial of S is denoted as $S(x)=s_0+s_1x+s_2x^2+\cdots+s_{2p^2-1}x^{2p^2-1}$.

2 Possible Values on Linear Complexity

In this section, we will present some general findings for q-ary sequences with the least period $2p^2$ and provide a comprehensive list of all possible linear complexity values for such sequences.

Lemma 1. *Let $S=(s_n)_{n=0}^{\infty}$ be a q-ary sequence with the least period $2p^2$. Here, p,q are both odd prime numbers ,$q<p$ and q is the primitive root module p^2. Let $\Phi_1(x)=1+x+x^2+\cdots+x^{p-1}$, $\Phi_1'(x)=1-x+x^2-\cdots+x^{p-1}$, $\Phi_2(x)=1+x^p+x^{2p}+\cdots+x^{(p-1)p}$ and $\Phi_2'(x)=1-x^p+x^{2p}-\cdots+x^{(p-1)p}$. Then in finite field $\mathbb{F}_q$, These four factors are all irreducible polynomials.*

Proof. Let q be a prime, n a positive integer with $gcd(q,n)=1$, and α a primitive n^{th} root of unity in some extension field of $\mathbb{F}_q$. The n^{th} cyclotomic polynomial over $\mathbb{F}_q$ is defined as

$$\Theta_n(x)=\prod_{\substack{i=1\\ gcd(n,i)=1}}^{n}\left(x-\alpha^i\right) \tag{3}$$

A simple argument show that $\Theta_{p^n}(x)=1+x^{p^{n-1}}+x^{2p^{n-1}}+\cdots+x^{(p-2)p^{n-1}}+x^{(p-1)p^{n-1}}=\frac{1-x^{p^n}}{1-x^{p^{n-1}}}$,and $\Theta_{2p^n}(x)=1-x^{p^{n-1}}+x^{2p^{n-1}}+\cdots-x^{(p-2)p^{n-1}}+x^{(p-1)p^{n-1}}=\frac{1+x^{p^n}}{1+x^{p^{n-1}}}$. Thus $\Theta_{p^n}(x)\Theta_{2p^n}(x)=1+x^{2p^{n-1}}+x^{4p^{n-1}}+\cdots+x^{2(p-1)p^{n-1}}=\frac{1-x^{2p^n}}{1-x^{2p^{n-1}}}$. Therefore, $x^{2p^2}-1=\left(x^2-1\right)\prod_{i=1}^{2}\Theta_{p^i}(x)\Theta_{2p^i}(x)=(x-1)(x+1)\Theta_p(x)\Theta_{2p}(x)\Theta_{p^2}(x)\Theta_{2p^2}(x)$.

According to Section 2. in [7] we know that $\Theta_p(x)$, $\Theta_{2p}(x)$, $\Theta_{p^2}(x)$, $\Theta_{2p^2}(x)$ are all irreducible polynomials. Let $\Phi_1(x)$ denote $\Theta_p(x)$, $\Phi_1'(x)$ denote $\Theta_{2p}(x)$, $\Phi_2(x)$ denote $\Theta_{p^2}(x)$ and $\Phi_2'(x)$ denote $\Theta_{2p^2}(x)$.we have $x^{p^2}-1=(x-1)\Phi_1(x)\Phi_2(x)$, $x^{p^2}+1=(x+1)\Phi_1'(x)\Phi_2'(x)$ and $x^{2p^2}-1=\left(x^{p^2}-1\right)\left(x^{p^2}+1\right)=(x-1)(x+1)\Phi_1(x)\Phi_1'(x)\Phi_2(x)\Phi_2'(x)$. □

Lemma 2. *Let $S=(s_n)_{n=0}^{\infty}$ be a q-ary sequence with the least period $2p^2$, the corresponding matrices as described above and $S^{2p^2}(x)=s_0+s_1x+s_2x^2+\cdots+s_{2p^2-1}x^{2p^2-1}$ be the generating polynomial of sequence S, thus , we have*

(i) $\Phi_i(x)\,|S^{2p^2}(x)$ if and only if $\Phi_i(x)\,|\mathfrak{A}_{(x)}^{(3)}$;

(ii) $\Phi_i'(x)\,|S^{2p^2}(x)$ if and only if $\Phi_i'(x)\,|\mathfrak{A}_{(x)}^{(4)}$;

Proof. The corresponding matrices $\mathfrak{A}_{(x)}^{(1)}$ and $\mathfrak{A}_{(x)}^{(2)}$ can be written as: $\mathfrak{A}_{(x)}^{(1)}=s_0+s_1x+s_2x^2+\cdots+s_{p^2-1}x^{p^2-1}$ and $\mathfrak{A}_{(x)}^{(2)}=s_{p^2}+s_{p^2+1}x+s_{p^2+2}x^2+\cdots+s_{2p^2-1}x^{p^2-1}$.Thus, $S^{2p^2}(x)$ can be written as: $S^{2p^2}(x)=\left(s_0+s_1x+s_2x^2+\cdots+s_{p^2-1}x^{p^2-1}\right)+x^{p^2}\left(s_{p^2}+s_{p^2+1}x+s_{p^2+2}x^2+\cdots+s_{2p^2-1}x^{p^2-1}\right)\triangleq\mathfrak{A}_{(x)}^{(1)}+x^{p^2}\mathfrak{A}_{(x)}^{(2)}$.

The expression can be reduced to 2 forms:

(i) $S^{2p^2}(x)=\left(\mathfrak{A}_{(x)}^{(1)}+\mathfrak{A}_{(x)}^{(2)}\right)+\left(x^{p^2}-1\right)\mathfrak{A}_{(x)}^{(2)}$;

(ii) $S^{2p^2}(x)=\left(\mathfrak{A}_{(x)}^{(1)}-\mathfrak{A}_{(x)}^{(2)}\right)+\left(x^{p^2}+1\right)\mathfrak{A}_{(x)}^{(2)}$;

We can get:

(i) since $\Phi_i(x)\,|\left(x^{p^2}-1\right)$, then $S^{2p^2}(x)\equiv\mathfrak{A}_{(x)}^{(1)}+\mathfrak{A}_{(x)}^{(2)}\,(mod\Phi_i(x))$,thus we can get that $\Phi_i(x)\,|S^{2p^2}(x)\Leftrightarrow\Phi_i(x)\,|\left(\mathfrak{A}_{(x)}^{(1)}+\mathfrak{A}_{(x)}^{(2)}\right)\Leftrightarrow\Phi_i(x)\,|\mathfrak{A}_{(x)}^{(3)}$;

(ii) since $\Phi_i'(x)\,|\left(x^{p^2}+1\right)$, then $S^{2p^2}(x)\equiv\mathfrak{A}_{(x)}^{(1)}-\mathfrak{A}_{(x)}^{(2)}\,(mod\Phi_i(x))$,thus we can get that $\Phi_i'(x)\,|S^{2p^2}(x)\Leftrightarrow\Phi_i'(x)\,|\left(\mathfrak{A}_{(x)}^{(1)}-\mathfrak{A}_{(x)}^{(2)}\right)\Leftrightarrow\Phi_i'(x)\,|\mathfrak{A}_{(x)}^{(4)}$;

□

The conclusion can also be applied to the combination of $(x-1)$ and $\Phi_i(x)$ or $(x+1)$ and $\Phi_i'(x)$.

Lemma 3. *Let $S=(s_n)_{n=0}^{\infty}$ be a q-ary sequence with the least period $2p^2$ and the corresponding matrices and polynomials as adescribed above, we have*

(i) $\Phi_2(x)\,|S^{2p^2}(x)$ if and only if each column of the matrix $\mathfrak{A}^{(3)}$ is in the form of $[k,k,k,\ldots,k,k]^T$, and k in each column does not have to be the same.

(ii) $\Phi_2'(x)\,|S^{2p^2}(x)$ if and only if each column of the matrix $\mathfrak{A}^{(4)}$ is in the form of $[k,-k,k,\ldots,-k,k]^T$, and k in each column does not have to be the same.

Proof. From the proof of Lemma 2 we know that $\Phi_2'(x)\,|S^{2p^2}(x)\Leftrightarrow\Phi_2'(x)\,|\mathfrak{A}_{(x)}^{(4)}$. Let $\mathfrak{A}_{(x)}^{(4)}=t_0+t_1x+\cdots+t_{p^2-1}x^{p^2-1}=\sum_{j=0}^{p-1}\sum_{l=0}^{p-1}t_{j+lp}x^{j+lp}=\sum_{j=0}^{p-1}\left(x^j\sum_{l=0}^{p-1}t_{j+lp}x^{lp}\right)$ and $\Phi_2'(x)=\sum_{i=0}^{p-1}(-1)^i x^{ip}$. Assume that $\Phi_2'(x)\,|\mathfrak{A}_{(x)}^{(4)}$, let $\mathfrak{A}_{(x)}^{(4)}=\Phi_2'(x)\left(h_0+h_1x+h_2x^2+\cdots+h_{p-1}x^{p-1}\right)$. Thus $\mathfrak{A}_{(x)}^{(4)}=\sum_{j=0}^{p-1}\left(h_j'x^j\sum_{l=0}^{p-1}(-1)^l x^{lp}\right)=\sum_{j=0}^{p-1}\left(x^j\sum_{l=0}^{p-1}(-1)^l h_j'x^{lp}\right)$, then we can get that $\Phi_2'(x)\,|\mathfrak{A}_{(x)}^{(4)}$ if and only if for $0\le j\le p-1$ and $0\le l\le p-1$, $s_{j+lp}=(-1)^l h_j'$. Then we derive for $0\le j,l\le p-1$, $(-1)^l s_{j+lp}=s_j$. The proof of the condition of $\Phi_2(x)\,|S^{2p^2}(x)$ is similar to above. □

Lemma 4. *Let $S=(s_n)_{n=0}^{\infty}$ be a q-ary sequence with the least period $2p^2$, then $\left(x^{p^2}+1\right) \nmid S(x)$.*

Proof. Let $S=\left(s_0, s_1, \ldots, s_{2p^2-1}\right)$ be arranged into matrix $\mathfrak{A}_S \triangleq \left[\begin{smallmatrix}\mathfrak{A}^{(1)}\\ \mathfrak{A}^{(2)}\end{smallmatrix}\right]$.

If $\left(x^{p^2}+1\right) | S(x)$, then the generating polynomial can be written as $S(x) = \left(x^{p^2}+1\right)\left(h_0+h_1x+h_2x^2+h_3x^3+\ldots+h_{p^2-1}x^{p^2-1}\right)$, for $0 \leqslant i < p^2-1$, let $h_i \subseteq \mathbb{F}_q$, then h_ix^i and $h_{i+p^2}x^{i+p^2}$ are included in $S(x)$, so we can get that in matrix $\mathfrak{A}_S \triangleq \left[\begin{smallmatrix}\mathfrak{A}^{(1)}\\ \mathfrak{A}^{(2)}\end{smallmatrix}\right]$, for $0 \leqslant i < p^2$, $S_i = S_{i+p^2}$, indicating $\mathfrak{A}^{(1)} = \mathfrak{A}^{(2)}$. Hence the period of the sequence S drops to p^2, which contradicts to the least period $2p^2$. So $\left(x^{p^2}+1\right) \nmid S(x)$. □

Lemma 5. *Let $S=(s_n)_{n=0}^{\infty}$ be a q-ary sequence with the least period $2p^2$, then $\Phi_2(x)\Phi_2'(x) \nmid S(x)$.*

Proof. The proof of the conditions of $\Phi_2(x)\Phi_2'(x) \nmid S(x)$ is similar to Lemma 4. In this situation, if $\Phi_2(x)\Phi_2'(x) \mid S(x)$, each bit of any column in matrix $\mathfrak{M}_S$ is the same, the sequence S drops to $2p$, which contradicts to the least period $2p^2$. So we can get $\Phi_2(x)\Phi_2'(x) \nmid S(x)$. □

Theorem 1. *Let $S=(s_n)_{n=0}^{\infty}$ be a q-ary sequence with the least period $2p^2$. If q is a primitive root modulo p^2, then the linear complexity of* S *satisfies one of the following cases:*

$$\begin{aligned} LC(S) \in \{&2p^2, 2p^2-1, 2p^2-2, 2p^2-p+1, 2p^2-p,\\ &2p^2-p-1, 2p^2-2p+2, 2p^2-2p+1,\\ &2p^2-2p, p^2+p, p^2+p-1, p^2+p-2,\\ &p^2+1, p^2, p^2-1, p^2-p+2, p^2-p+1,\\ &p^2-p\} \end{aligned}$$

Proof. According to Lemma 4 and Lemma 5, we know $\left(x^{p^2}+1\right) \nmid S(x)$ and $\Phi_2(x)\Phi_2'(x) \nmid S(x)$.So we can get that for a sequencese with the least period $2p^2$, its generating polynomial should not have $\left(x^{p^2}+1\right)$ or $\Phi_2(x)\Phi_2'(x)$. Thus the generating polynomial of the sequence is one of the subfactor of $(x-1)(x+1)\Phi_1(x)\Phi_1(x)'\Phi_2(x)\Phi_2(x)'$ that do not contain $(x+1)\Phi_1'(x)\Phi_2'(x)$ or $\Phi_2(x)\Phi_2'(x)$.

There are 44 different generating polynomials in total, and the minimal polynomial of S is $x^{2p^2}-1$ divided by one of the forty-four items. Hence, the linear complexity of the sequence S satisfies one of the following eighteen items:

$$\begin{aligned} LC(S) \in \{&2p^2, 2p^2-1, 2p^2-2, 2p^2-p+1, 2p^2-p,\\ &2p^2-p-1, 2p^2-2p+2, 2p^2-2p+1,\\ &2p^2-2p, p^2+p, p^2+p-1, p^2+p-2,\\ &p^2+1, p^2, p^2-1, p^2-p+2, p^2-p+1,\\ &p^2-p\} \end{aligned}$$

The period of the sequence remains $2p^2$ as long as its generating polynomial does not contain $\left(x^{p^2}+1\right)$ or $\Phi_2(x)\Phi_2'(x)$. According to our classification, the linear complexity of the sequence reaches its minimum value p^2-p when its generating polynomial is $(x-1)(x+1)\Phi_1(x)\Phi_1'(x)\Phi_2(x)$. So far,we have obtained all the values and the lower bounds of the linear complexity of the sequence S. □

3 *K*-error Linear Complexity

In this section, we will examine the k-error linear complexity of sequence S using the classification outlined in Theorem 1.We will then introduce an algorithm for computing the k-error linear complexity according to the rules we have developed. This algorithm will be presented in Section 3.1. To demonstrate how to apply the algorithm, we will randomly generate a sequence and use the algorithm to obtain the desired k-error linear complexity. This example will be presented in Section 3.2.

3.1 Algorithm to Get the *k*-error Linear Complexity

Compared to the binary or q-ary sequence with period p^2 and the binary sequence with period $2p^2$, the $q-ary$ sequence with period $2p^2$ that we study is more complex, and its generating polynomial consists of six irreducible polynomials:$(x-1)$, $(x+1)$, $\Phi_1(x)$, $\Phi_1'(x)$, $\Phi_2(x)$ and $\Phi_2'(x)$, so its analysis process is more complicated and there are more conditions to consider.

According to Theorem 1, the maximum common divisor between the generating polynomial and $x^{2p^2}-1$ must be one of the forty-four items. So we can get forty-four different minimal polynomials. Arranging the sequences generated by different generating polynomials into matrix forms, we can see that their matrices have different characteristics, but some of the sequences generated by different generating polynomials share the same linear complexity, which can be proved in Theorem 1.

Therefore, when we discuss the k-error linear complexity of S, we need to analyze which matrix characteristic is in each case, get the minimum number of bits that the current matrix needs to be changed for the target matrix, and get the minimum value of all minimums with the same linear complexity to get the desired final result.

Next, we need to introduce some symbols to represent some features of the matrices.

Let X_i denote the i-th column in the matrix X, $wt_l(X_i)$ denote the number of occurrences of l in X_i, $wt_l'(X_i)$ denote the number of elements where the even bits are l and the odd bits are $q-l$ in X_i, $ct(X)$ denote the element value used in X. For example, $ct(wt_l(X_i))$ denote l finally used in $wt_l(X_i)$.

Let $\mathfrak{A}_i^{(n)}$ denote the i^{th} column of $\mathfrak{A}^{(n)}$ and $\mathfrak{A}_i'^{(n)}$ denote the i^{th} element of $\mathfrak{A}^{(n)}$.

Let $\sum(X_i)$ denote the sum of each element in X_i of the matrix and $\sigma(X_i)$ denote the result of subtracting the sum of the even bits from the sum of the odd bits in X_i.

Let $m_{1j} = \sum_{\substack{0\leqslant i<2p \\ \sum(M_i)\equiv j(\bmod q)}} 1$, $m_{2j} = \sum_{\substack{0\leqslant i<2p \\ \sum(M_i)\equiv j(\bmod q) \\ i\equiv 0(\bmod 2)}} 1$,

$m_{3j} = \sum_{\substack{0\leqslant i<2p \\ \sum(M_i)\equiv q-j(\bmod q) \\ i\equiv 1(\bmod 2)}} 1$,

$$m_4 = \sum_{0\leqslant i<p}\left(\max_{0\leqslant j<q}\left\{\sum_{\substack{0\leqslant l<p \\ \mathfrak{A}'^{(4)}_{(i+lp)}=j \\ l\equiv 0(\bmod 2)}} 1 + \sum_{\substack{0\leqslant l<p \\ \mathfrak{A}'^{(4)}_{(i+lp)}=q-j \\ l\equiv 1(\bmod 2)}} 1\right\}\right),$$

$m_{5j} = \sum_{\substack{0\leqslant i<p \\ \sum\left(\mathfrak{A}_i^{(3)}\right)\equiv j(\bmod q)}} 1$,

$$m_6 = \max\left\{\sum_{\substack{0\leqslant j<q \\ \sigma\left(ct\left(wt'_l\left(\mathfrak{A}_j^{(4)}\right)\right)\right)\equiv 0(\bmod q)}} wt'_l\left(\mathfrak{A}_j^{(4)}\right)\right\},$$

$m_7 = \sum_{\substack{0\leqslant i<p \\ \sum\left(\mathfrak{A}_i^{(3)}\right)\equiv 0(\bmod q)}} 1$,

$m_{8j} = \sum_{\substack{0\leqslant i<2p \\ \sum(M_i)\equiv j(\bmod q) \\ i\equiv 0(\bmod 2)}} 1 + \sum_{\substack{0\leqslant i<2p \\ \sum(M_i)\equiv q-j(\bmod q) \\ i\equiv 1(\bmod 2)}} 1$,

$m_9 = \sum_{\substack{0\leqslant i<p \\ \sum(M_i)+\sum(M_{i+p})\equiv 0(\bmod q)}} 1$,

Now we discuss the k-error linear complexity of S.

Theorem 2. *Let $S=(s_n)_{n=0}^{\infty}$ be a q-ary sequence with the least period $2p^2$. Let the corresponding $p\times 2p$ matrix be $\mathfrak{M}_S=[M_0,M_1,\cdots,M_{2p-1}]$, the corresponding $2p\times p$ matrix be $\mathfrak{A}_S \triangleq \left[\frac{\mathfrak{A}^{(1)}}{\mathfrak{A}^{(2)}}\right]$, and the corresponding $p\times p$ matrix be $\mathfrak{A}^{(3)}=\mathfrak{A}^{(1)}+\mathfrak{A}^{(2)} \triangleq \left[\mathfrak{A}_0^{(3)},\mathfrak{A}_1^{(3)},\cdots,\mathfrak{A}_{p-1}^{(3)}\right]$ and $\mathfrak{A}^{(4)}=\mathfrak{A}^{(1)}-\mathfrak{A}^{(2)} \triangleq \left[\mathfrak{A}_0^{(4)},\mathfrak{A}_1^{(4)},\cdots,\mathfrak{A}_{p-1}^{(4)}\right]$, the characteristic polynomial of S be $S(x)$.*

Algorithm 1 Computing the k-error linear complexity of a sequence with period $2p^2$ over $\mathbb{F}_q$

Require: Fuction $lstchange(S,h(x))$ returns the smallest number to change the sequence to the $h(x)$ type. Variables k_i are initialized to be $2p^2$, in every computation of k_i, if the linear complexity correspond to $h(x)$ is greater than l, this step should be ignored.
$l=LC(S)$
After figuring out the linear complexity l of the sequence S by algorithm 1 in [18], all the items whose linear complexities are greater than l should be deleted.

if $2p^2-2p\leqslant l\leqslant 2p^2$ **then**
  $flag=1$
end if
if $p^2+p-2\leqslant l\leqslant p^2+p$ **then**
  $flag=2$
end if
if $p^2-1\leqslant l\leqslant p^2+1$ **then**
  $flag=3$
end if
if $2p\leq l\leqslant p^2-p+2$ **then**
  $flag=4$
end if
if $flag=1$ **then**
  $k_0=0$
  $k_1=\min(lstchange(S,x-1),lstchange(S,x+1))$
  $k_2=lstchange(S,x^2-1)$
  $j=\min(lstchange(S,\Phi_1(x)),lstchange(S,\Phi'_1(x)))$
  if $j=lstchange(S,\Phi_1(x))$ **then**
    $k_3=lstchange(S,\Phi_1(x))$
    $k_4=\min(lstchange(S,(x-1)\Phi_1(x)),lstchange(S,(x+1)\Phi_1(x)))$
    $k_5=lstchange(S,(x-1)(x+1)\Phi_1(x))$
  end if
  if $j=lstchange(S,\Phi'_1(x))$ **then**
    $k_3=\min(k_3,lstchange(S,\Phi'_1(x)))$
    $k_4=\min(k_4,lstchange(S,(x-1)\Phi'_1(x)),lstchange(S,(x+1)\Phi'_1(x)))$
    $k_5=\min(k_5,lstchange(S,(x-1)(x+1)\Phi_1(x)))$
  end if
  $k_6=lstchange(S,\Phi_1(x)\Phi'_1(x))$
  $k_7=\min(lstchange(S,(x-1)\Phi_1(x)\Phi'_1(x)),lstchange(S,(x+1)\Phi_1(x)\Phi'_1(x)))$
  $k_8=lstchange(S,(x-1)(x+1)\Phi_1(x)\Phi'_1(x))$
  $flag=2$
end if
if $flag=2$ **then**
  $j=\min(lstchange(S,\Phi_2(x)),lstchange(S,\Phi'_2(x)))$
  if $j=lstchange(S,\Phi_2(x))$ **then**
    $k_9=lstchange(S,\Phi_2(x))$
    $k_{10}=\min(lstchange(S,(x-1)\Phi_2(x)),lstchange(S,(x+1)\Phi_2(x)))$
    $k_{11}=lstchange(S,(x-1)(x+1)\Phi_2(x))$
  end if
  if $j=lstchange(S,\Phi'_2(x))$ **then**
    $k_9=\min(k_9,lstchange(S,\Phi'_2(x)))$
    $k_{10}=\min(k_{10},lstchange(S,(x-1)\Phi'_2(x)),lstchange(S,(x+1)\Phi'_2(x)))$
    $k_{11}=\min(k_{11},lstchange(S,(x-1)(x+1)\Phi_2(x)))$
  end if
  $flag=3$
end if
if $flag=3$ **then**
  $j=\min(lstchange(S,\Phi_1(x)\Phi_2(x)),$
    $lstchange(S,\Phi'_1(x)\Phi_2(x)),$
    $lstchange(S,\Phi_1(x)\Phi'_2(x)),$
    $lstchange(S,\Phi'_1(x)\Phi'_2(x))$
  if $j=lstchange(S,\Phi_1(x)\Phi_2(x))$ **then**
    $k_{12}=lstchange(S,\Phi_1(x)\Phi_2(x))$
    $k_{13}=\min(lstchange(S,(x-1)\Phi_1(x)\Phi_2(x)),lstchange(S,(x+1)\Phi_1(x)\Phi_2(x)))$
    $k_{14}=lstchange(S,(x-1)\ (x+1)\Phi_1(x)\Phi_2(x))$
  end if

if $j = lstchange(S, \Phi_1'(x)\Phi_2(x))$ **then**
$k_{12} = \min(k_{12}, lstchange(S, \Phi_1'(x)\Phi_2(x)))$
$k_{13} = \min(k_{13}, lstchange(S, (x-1)\Phi_1'(x)\Phi_2(x))$
$, lstchange(S, (x+1)\Phi_1'(x)\Phi_2(x)))$
$k_{14} = \min(k_{14}, lstchange(S, (x^2-1)\Phi_1'(x)\Phi_2(x)))$
end if
if $j = lstchange(S, \Phi_1(x)\Phi_2'(x))$ **then**
$k_{12} = \min(k_{12}, lstchange(S, \Phi_1(x)\Phi_2'(x)))$
$k_{13} = \min(k_{13}, lstchange(S, (x-1)\Phi_1(x)\Phi_2'(x))$
$, lstchange(S, (x+1)\Phi_1(x)\Phi_2'(x)))$
$k_{14} = \min(k_{14}, lstchange(S, (x^2-1)\Phi_1(x)\Phi_2'(x)))$
end if
if $j = lstchange(S, \Phi_1'(x)\Phi_2'(x))$ **then**
$k_{12} = \min(k_{12}, lstchange(S, \Phi_1'(x)\Phi_2'(x)))$
$k_{13} = \min(k_{13}, lstchange(S, (x-1)\Phi_1'(x)\Phi_2'(x)))$
end if
$flag = 4$
end if
if $flag = 4$ **then**
$j = \min(lstchange(S, \Phi_1(x)\Phi_1'(x)\Phi_2(x))$
$, lstchange(S, \Phi_1(x)\Phi_1'(x)\Phi_2'(x))$
if $j = lstchange(S, \Phi_1(x)\Phi_1'(x)\Phi_2(x))$ **then**
$k_{14} = lstchange(S, \Phi_1(x)\Phi_1'(x)\Phi_2(x)))$
$k_{15} = \min(lstchange(S, (x-1)\Phi_1(x)\Phi_1'(x)\Phi_2(x))$
$, lstchange(S, (x+1)\Phi_1(x)\Phi_1'(x)\Phi_2(x)))$
$k_{16} = lstchange(S, (x^2-1)\Phi_1(x)\Phi_1'(x)\Phi_2(x)))$
end if
if $j = lstchange(S, \Phi_1(x)\Phi_1'(x)\Phi_2'(x))$ **then**
$k_{14} = \min(k_{14}, lstchange(S, \Phi_1(x)\Phi_1'(x)\Phi_2'(x))))$
$k_{15} = \min(k_{15}, lstchange(S, (x-1)\Phi_1(x)\Phi_1'(x)\Phi_2'(x)))$
end if
end if

According to the algorithm 1, for k_i and k_{i+1}, they are adjacent and the linear complexity of k_i is greater. The following rules should be applied to get the desired k-error linear complexity.

Rules to get desired k-error linear complexity

1. Define the item k_i as the line correspongding to $k_i < k < k_{i+1}$
2. Calculate each value of k separately by the algorithm above;
3. If $k_{i+1} > k_i$, item k_i is deleted and k_{i+1} is retained;
4. If $k_i = k_{i+1}$, item k_i is deleted and k_{i+1} is retained;
5. If $k_{i+1} < k_i$, items from k_{j+1} to k_i are deleted, here k_j is the first k that is less than k_{i+1} and $j < i$.

By arranging the reserved k_i and the corresponding linear complexity in ascending order, we can finally obtain the linear complexity segmented expression of the sequence.

Proof. Let β denote how many bits we change in the sequence. If the linear complexity of the sequence is $p^2 - p$, it is the minimum of the linear complexity of the sequence S^{2p^2}. Therefore, changing any bits of the sequence will not cause a decrease in the linear complexity as long as the period of the sequence does not decrease. So we consider how many terms changed in S^{2p^2} will cause the period to decrease. We can see that the period of s will drop to $2p$ when each column of matrix $\mathfrak{M}_S$ is $(k, k, \ldots, k)^T$, so we only need to change $\left(p - \max_{0 \leqslant l < q} \{wt_l(M_i)\}\right)$ terms for each column.

Based on the observation and derivation of different sequences generated by different generating polynomials , we can find that if $\Phi_1(x)\Phi_1'(x) \mid S^{2p^2}(x)$, then the sums of each element in each odd column in the matrix $\mathfrak{M}_S$ are equal, and the same for the even columns. So we take $\mu = 2p - \max_{0 \leqslant j < q} \{n_{2j}\} - \max_{0 \leqslant j < q} \{n_{3j}\}$ to satisfy this condition, when $\beta \geq \mu$, the linear complexity of sequence $LC(s) \leq 2p^2 - 2p + 2$. When $(x+1)\Phi_1(x)\Phi_1'(x) \mid S^{2p^2}(x)$, the sums of the elements in each column of the matrix are equal. When $(x-1)\Phi_1(x)\Phi_1'(x) \mid S^{2p^2}(x)$, the sums of each element of each odd column in the matrix are equal, and the same for even columns, and the sum of these two numbers is 0. So, we take $\alpha_1 = 2p - \max_{0 \leqslant j < q} \{m_{1j}\}$, $\alpha_2 = 2p - \max_{0 \leqslant j < q} \{n_{2j} + n_{3j}\}$ and $k = \min\{\alpha_1, \alpha_1\}$ to satisfy the condition. When $\beta \geq k$, the linear complexity of sequence $LC(s) \leq 2p^2 - 2p + 1$.

According to Theorem 1 we can know that the generating polynomial is obtained by combining the six polynomials $(x-1)$, $(x+1)$, $\Phi_1(x)$, $\Phi_1'(x)$, $\Phi_2(x)$ and $\Phi_2'(x)$ under the constraints of $\left(x^{p^2}+1\right) \nmid S(x)$ and $(\Phi_2(x)\Phi_2'(x)) \nmid S(x)$. They all represent different matrix characteristics. $(x-1)$ represents that the sum of each bit in the matrix is 0; $(x+1)$ represents that the sum of odd bits and sum of even bits in the matrix are equal; $\Phi_1(x)$ represents that in the matrix $\mathfrak{A}^{(3)}$, the sums of each column are equal; $\Phi_1'(x)$ represents that in the matrix $\mathfrak{A}^{(4)}$, the differences between the sum of even bits and the sum of odd bits in each column should be equal; $\Phi_2(x)$ represents that in $\mathfrak{A}^{(3)}$, the elements of each column share the same value; and $\Phi_2'(x)$ represents that in matrix $\mathfrak{A}^{(4)}$, the even and the odd bits of each column are the same value respectively, and their sum is 0. Their combination will bring new characteristics to the matrix, for example,$(x-1)(x+1)$ represents that the sum of the odd bits and the sum of the even bits of the matrix are equal, and their sum is 0. Since q is a prime, their sums must both be 0.

Based on the different generating polynomials, we obtain different sequences with different matrix characteristics and find the minimum number of bits that need to be changed for the current matrix to obtain the specific characteristic, and combining the conditions of the same linear complexity, we obtain the most general conclusion. Then, using the rules described in Algorithm 1., we can obtain the k-error linear complexity for a given sequence. □

3.2 Numerical Example

In this section, we will randomly generate a q-ary sequence to illustrate how to use the algorithm we devel-

oped in Section 3.1 to obtain the desired k-error linear complexity. Specifically, we will demonstrate how to apply the algorithm to compute the k-error linear complexity of the generated sequence. This example will provide a step-by-step explanation of the algorithm and serve as a guide for applying it to other sequences. Let S be a 3-ary sequence of period $T = 2 \times 5^2$, with S^T = 11121 21010 12021 22112 11120 02001 02002 11100 11112 02100, then the corresponding $p \times p$ matrices are $\mathfrak{A}^{(3)} = \mathfrak{A}^{(1)} + \mathfrak{A}^{(2)} = \begin{bmatrix} 1 & 0 & 1 & 2 & 2 \\ 2 & 0 & 0 & 1 & 2 \\ 2 & 0 & 1 & 2 & 1 \\ 0 & 0 & 2 & 2 & 1 \\ 1 & 0 & 2 & 2 & 0 \end{bmatrix}$ and $\mathfrak{A}^{(4)} = \mathfrak{A}^{(1)} - \mathfrak{A}^{(2)} = \begin{bmatrix} 1 & 2 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 & 1 \\ 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 2 & 0 \end{bmatrix}$,and the corresponding $p \times 2p$ matrix is $\mathfrak{M}_s = \begin{bmatrix} 1 & 1 & 1 & 2 & 1 & 2 & 1 & 0 & 1 & 0 \\ 1 & 2 & 0 & 2 & 1 & 2 & 2 & 1 & 1 & 2 \\ 1 & 1 & 1 & 2 & 0 & 0 & 2 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & 2 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 2 & 0 & 2 & 1 & 0 & 0 \end{bmatrix}$, the sum of odd items is 2 and the sum of even items is 1.

Let $\mu_1 = p^2 - \max\limits_{0 \leqslant j < q} \{m_{8j}\}$, $\mu_2 = \mu_1 + 2(p - m_9)$, $\mu_3 = \mu_1 + \mu_{20}$,

$$\mu_4 = \begin{cases} 0, & \text{if } \sum\limits_{\substack{0 \leqslant i < 2p^2 \\ i \equiv 0 (\bmod 2)}} s_i \equiv \sum\limits_{\substack{0 \leqslant i < 2p^2 \\ i \equiv 1 (\bmod 2)}} s_i \equiv 0 \,(\bmod\ q) \\ 1, & \text{if } \sum\limits_{\substack{0 \leqslant i < 2p^2 \\ i \equiv 0 or 1 (\bmod 2)}} s_i \equiv 0 \,(\bmod\ q) \\ 2, & \text{else.} \end{cases},$$

$\mu_5 = p^2 - m_6$, $\mu_6 = \mu_5 + 2\mu_9$,

$$\mu_7 = \begin{cases} 0, & \text{if } \sum\limits_{\substack{0 \leqslant i < 2p^2 \\ i \equiv 0 (\bmod 2)}} s_i - \sum\limits_{\substack{0 \leqslant i < 2p^2 \\ i \equiv 1 (\bmod 2)}} s_i \equiv 0 \,(\bmod\ q) \\ 1, & \text{else.} \end{cases},$$

$\mu_8 = \sum\limits_{0 \leqslant j < p} (p - m_4)$, $\mu_9 = p - m_7$,

$\mu_{10} = \mu_8 + 2\mu_9$, $\mu_{11} = p - \max\limits_{0 \leqslant j < q} \{m_{5j}\}$, $\mu_{12} = \mu_5 + 2\mu_{11}$,

$$\mu_{13} = \begin{cases} 0, & \text{if } \sum\limits_{\substack{0 \leqslant i < 2p^2 \\ i \equiv 0 (\bmod 2)}} s_i + \sum\limits_{\substack{0 \leqslant i < 2p^2 \\ i \equiv 1 (\bmod 2)}} s_i \equiv 0 \,(\bmod\ q) \\ 1, & \text{else.} \end{cases},$$

$\mu_{14} = \mu_8 + 2\mu_{11}$, $\mu_{15} = \mu_5 + \mu_4$, $\mu_{16} = \mu_8 + 2\mu_{13}$, $\mu_{17} = 2p - m_{10}$, $\mu_{18} = 2p - \max\limits_{0 \leqslant j < q} \{m_{1j}\}$, $\mu_{19} = 2p - \max\limits_{0 \leqslant j < q} \{m_{2j} + m_{3j}\}$, $\mu_{20} = 2p - \max\limits_{0 \leqslant j < q} \{m_{2j}\} - \max\limits_{0 \leqslant j < q} \{m_{3j}\}$, $\mu_{21} = \mu_9 + 2\mu_4$, $\mu_{22} = \mu_{11} + 2\mu_7$ $\mu_{23} = \sum\limits_{0 \leqslant i < p} \left(p - wt_0\left(\mathfrak{A}_i^{(3)}\right)\right)$, $\mu_{24} = \mu_{23} + \mu_{17}$, $\mu_{25} = \sum\limits_{0 \leqslant i < 2p} \left(p - \max\limits_{0 \leqslant l < q} \{wt_l(M_i)\}\right)$, these items are used to compute the funcion $lstchange(s, h(x))$ in the algorithm.

Analyzing $\mathfrak{A}^{(3)}$, we find that the sums of each column of $\mathfrak{A}^{(3)}$ are 0. Therefore, we can conclude that the generating polynomial of the sequence is $(x-1)\Phi_1(x)$. Then, according to the rules in Algorithm 1, k_0 to k_3 should be ignored, and $k_4 = lstchange(S, (x-1)\Phi_1(x)) = \mu_9 = 0$. Then we can compute $k_5 = lstchange(S, x^2 - 1\Phi_1(x^2)) = \mu_{21} = 2$(we can increase and decrease 1 by the corresponding bits s_i and s_{i+p^2}, here i is an odd number, respectively), next from our computation we can get that $k_6 = \mu_{20} = 6$, $k_7 = \min(\mu_{19}, \mu_{18}) = 6$, $k_8 = \mu_{17} = 6$, $k_9 = \mu_8 = 9$, $k_{10} = \min(\mu_{16}, \mu_5) = 9$, $k_{11} = \mu_{15} = 17$, $k_{12} = \mu_{14} = 13$, $k_{13} = \min(\mu_{10}, \mu_{12}) = 15$, $k_{14} = \mu_6 = 12$, $k_{15} = \mu_3 = 15$, $k_{16} = \mu_2 = 15$, $k_{17} = \mu_{24} = 19$, $k_{18} = \mu_{25} = 21$. And the branches we choose are $\Phi_2(x)$, $\Phi_1(x)\Phi_2(x)'$ and $\Phi_1(x)\Phi_1(x)'\Phi_2(x)'$.

Applying the rules in Algorithm to all k, we can know k_6, k_7, k_9, k_{11}, k_{12}, k_{13} and k_{15} should be deleted so the k-error linear complexity segmented expression of the sequence is $LC_k(s) = \begin{cases} 2p^2 - p, & \text{if } k_4 \leqslant k < k_5 \\ 2p^2 - p - 1, & \text{if } k_5 < k \leqslant k_8 \\ 2p^2 - 2p, & \text{if } k_8 \leqslant k < k_{10} \\ p^2 + p - 1, & \text{if } k_{10} \leqslant k < k_{14} \\ p^2 - 1, & \text{if } k_{14} \leqslant k < k_{16} \\ p^2 - p + 1, & \text{if } k_{16} \leqslant k < k_{17} \\ p^2 - p, & \text{if } k_{17} \leqslant k < k_{18} \\ \leqslant 2p, & \text{if } k_{18} \leqslant k \end{cases}$.

Then it is easy to get the k-error linear complexity segmented expression:

$$LC_k(s) = \begin{cases} 45, & \text{if } 0 \leqslant k < 2 \\ 44, & \text{if } 2 \leqslant k < 6 \\ 40, & \text{if } 6 \leqslant k < 9 \\ 28, & \text{if } 9 \leqslant k < 12 \\ 24, & \text{if } 12 \leqslant k < 15 \\ 21, & \text{if } 15 \leqslant k < 19 \\ 20, & \text{if } 19 \leqslant k < 21 \\ \leq 10, & \text{if } 21 \leqslant k \end{cases}.$$

We ran the program for algorithm 2 from [18] and compared its results with our own computations of the k-error linear complexity of sequence s. We found that the algorithm produced the same results as our computation.

To further test the accuracy of our method, we randomly generated additional sequences using different generating polynomials. In all cases, our computations were consistent with our proposed algorithm. These results demonstrate the effectiveness and reliability of our approach.

4 *K*-error Sequences

In this section, we will introduce how to compute the number of k-error sequences of a sequence by the matrix method, and analyze the case when the linear complexity of the sequence decreases to about p^2, and it is closer to an all-0 matrix after arranging it into a $\mathfrak{A}_3$-matrix , this will be presented in Section 4.1. We will then give a specific example to demonstrate the correctness of the method, this will be presented in Section 4.2.

4.1 Get the Number of k-error Sequences

In this section, we will introduce a new method to compute the number of k-error sequences of a sequence based on the different matrix characteristics of the sequence at different linear complexities.

First, according to Theorem 2, we can know how many bits we should change, which generating polynomial the current sequence corresponds to and what characteristics the corresponding matrix should have. Then, to change the initial sequence to the target sequence, we can find out which changes are required at which positions in the matrix. Finally, we can obtain the number of k_i-error sequences and all k_i-error sequences.

Let $\mu_{26} = \mu_{23} + 2\mu_4$, $\mu_{27} = \mu_{23} + 2\mu_{13}$.

Theorem 3. *Let $S = (s_n)_{n=0}^{\infty}$ be a q-ary sequence with the least period $2p^2$, and the corresponding matrices and polynomials as described above, we have*

(i) $\beta_1 = \sum_{0 \leqslant i < p} \left(p - wt_0\left(\mathfrak{A}_i^{(3)}\right)\right)$,

(ii) Suppose $\gcd\left(x^{2p^2}-1, S(x)\right)$ *is* $(x-1)\Phi_1(x)\Phi_2(x)$, *then the matrix* $\mathfrak{A}^{(3)}$ *consisted of this sequence is an all-0 matrix, and we should change μ_1 bits to get it.If μ_1 is chosen to be k_{13}, then the number of k_{13}-error sequences should be 2^{β_1};*

(iii) Suppose $\gcd\left(x^{2p^2}-1, S(x)\right)$ *is* $(x-1)(x+1)\Phi_1(x)\Phi_2(x)$, *then the matrix* $\mathfrak{A}^{(3)}$ *consisted of this sequence is an all-0 matrix, the sum of the odd bits and the sum of even bits are both 0, and we should change μ_{26} bits to get it. If μ_{26} is chosen to be k_{14}, then the number of k_{14}-error sequences should be $2^{\beta_1} \times p^{\mu_4}$;*

(iv) Suppose $\gcd\left(x^{2p^2}-1, S(x)\right)$ *is* $(x-1)\Phi_1(x)\Phi_1'(x)\Phi_2(x)$, *then the matrix* $\mathfrak{A}^{(3)}$ *consisted of this sequence is an all-0 matrix, and the sums of the even and odd columns in the matrix $\mathfrak{M}_s$ are respectively equal and their sum is 0 (in the modulo q operation), and we should change μ_{27} bits to get it.If μ_{27} is chosen to be k_{16}, then the number of k_{16}-error sequences should be $2^{\beta_1} \times p^{\mu_{20}/2}$;*

(v) Suppose $\gcd\left(x^{2p^2}-1, S(x)\right)$ *is* $(x-1)(x+1)\Phi_1(x)\Phi_1'(x)\Phi_2(x)$, *then the matrix* $\mathfrak{A}^{(3)}$ *consisted of this sequence is an all-0 matrix and the sums of each column in matrix $\mathfrak{M}_s$ are all 0, and we should change μ_{24} i.e. k_{17} bits to get it, then the number of k_{17}-error sequences should be $2^{\beta_1} \times p^{m_{10}/2}$.*

Proof. According to Theorem 2, we know that when the generating polynomial contains

(i) $(x-1)\Phi_1(x)\Phi_2(x)$, then the matrix $\mathfrak{A}^{(3)}$ consisting of the sequence is an all-0 matrix, also in matrix $\mathfrak{M}_s$, the sum of each element in i-th column and the sum of each element in the $(i+p)$-th column sum to 0(in the modulo q operation), and the sum of odd and even bits in the matrix is 0;

(ii) $(x-1)(x+1)$, then the sum of the odd bits and the sum of even bits of the matrix are equal, and their sum is 0;

(iii) $\Phi_1(x)\Phi_1'(x)$, then the sums of each element in each odd column in the matrix $\mathfrak{M}_S$ are equal, and the same for the even columns.

In order to achieve the desired matrix characteristics, we need to first change the sequence so that it satisfies $(x-1)\Phi_1(x)\Phi_2(x) \mid S(x)$. So we just need to find every bit in the matrix $\mathfrak{A}^{(3)}$ that is not 0, for example, if $\mathfrak{A}_i'^{(3)} = q_1$, then $q - q_1$ needs to be added to either s_i or $s_{(i+p)}$ (under the mod q operation), so 2^{μ_1} bits needs to be changed.

If the sequence is expected to satisfy $(x-1)(x+1)\Phi_1(x)\Phi_2(x)$, we need to determine whether the sum of the even bits and the sum of the odd bits of the changed sequence are both 0. If not, it can be seen that the sums of the even and the odd bits are q_1 and $q-q_1$ respectively at this time, and we need to change the matrix $\mathfrak{A}^{(3)}$ with each bit of it kept as 0. We can choose any bit of $\mathfrak{A}^{(3)}$ like $\mathfrak{A}_i'^{(3)}$. Then add $q - q_1$ to the even element and q_1 to the odd element in s_i and $s_{(i+p)}$, so that the sum of the even and odd bits of the sequence is 0 under the condition that each bit of the matrix $\mathfrak{A}^{(3)}$ is 0.

Acoording to Theorem 2, β_1 denotes the number of bits in matrix $\mathfrak{A}^{(3)}$ that are not 0, and μ_4 denotes whether the sum of even bits and the sum of odd bits of the sequence are both 0. So we can get the number of k_{16}-error sequences should be $2^{\beta_1} \times p^{\mu_4}$;

The proof of the conditions of $(x-1)\Phi_1(x)\Phi_1'(x)\Phi_2(x)$ and $(x-1)(x+1)\Phi_1(x)\Phi_1'(x)\Phi_2(x)$ is similar to above. The other cases are studied in the same way as in Theorem 4. □

4.2 Numerical Example

Let S be a 3-ary sequence of period $T = 2 \times 5^2$ with S^T = 21210 21020 21202 10122 11122 12120 12010 12101 20211 22211, then the corresponding $2p \times p$ matrix is $\mathfrak{A}_s = \begin{bmatrix} 2&1&2&1&0\\ 2&1&0&2&0\\ 2&1&2&0&2\\ 1&0&1&2&2\\ 1&1&1&2&2\\ 1&2&1&2&0\\ 1&2&0&1&0\\ 1&2&1&0&1\\ 2&0&2&1&1\\ 2&2&2&1&1 \end{bmatrix} \triangleq \begin{bmatrix} \mathfrak{A}^{(1)} \\ \mathfrak{A}^{(2)} \end{bmatrix}$, the corresponding $p \times p$ matrices are $\mathfrak{A}^{(3)} = \mathfrak{A}^{(1)} + \mathfrak{A}^{(2)} = \begin{bmatrix} 0&0&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0 \end{bmatrix}$ and $\mathfrak{A}^{(4)} = \mathfrak{A}^{(1)} -$

$\mathfrak{A}^{(2)} = \begin{bmatrix} 1 & 2 & 1 & 2 & 0 \\ 1 & 2 & 0 & 1 & 0 \\ 1 & 2 & 1 & 0 & 1 \\ 2 & 0 & 2 & 1 & 1 \\ 2 & 2 & 2 & 1 & 1 \end{bmatrix}$, and the corresponding $p \times 2p$ matrix is $\mathfrak{M}_s = \begin{bmatrix} 2 & 1 & 2 & 1 & 0 & 2 & 1 & 0 & 2 & 0 \\ 2 & 1 & 2 & 0 & 2 & 1 & 0 & 1 & 2 & 2 \\ 1 & 1 & 1 & 2 & 2 & 1 & 2 & 1 & 2 & 0 \\ 1 & 2 & 0 & 1 & 0 & 1 & 2 & 1 & 0 & 1 \\ 2 & 0 & 2 & 1 & 1 & 2 & 2 & 2 & 1 & 1 \end{bmatrix}$.

According to Theorem 3, the generating polynomial of the sequence contains $(x-1)\Phi_1(x)\Phi_2(x)$. Therefore, after arranging the sequence into a $\mathfrak{A}^{(3)}$-matrix, each bit is 0. According to our computation, the sum of the even bits of the sequence is 1 , the sum of the odd bits of the sequence is 2, $\mu_4 = 2$, $\mu_{20} = 4$, $m_{10} = 10$ and the k-error linear complexity of the sequence is $LC_k(S) = \begin{cases} 25, & \text{if } 0 \leqslant k < 2 \\ 24, & \text{if } 2 \leqslant k < 4 \\ 21, & \text{if } 4 \leqslant k < 10 \\ 20, & \text{if } 10 \leqslant k < 22 \\ \leqslant 10, & \text{if } 22 \leqslant k \end{cases}$. According to the computation, when the linear complexity decreases to 24, the generating polynomial of the sequence after changing 2 bits is $(x-1)(x+1)\Phi_1(x)\Phi_2(x)$. When the linear complexity decreases to 21, the generating polynomial of the sequence after changing 4 bits is $(x-1)\Phi_1(x)\Phi_1'(x)\Phi_2(x)$. When the linear complexity decreases to 20, the generating polynomial of the sequence after changing 10 bits is $(x-1)(x+1)\Phi_1(x)\Phi_1'(x)\Phi_2(x)$. When the linear complexity is less than 10, the generating polynomial of the sequence after changing 22 bits is $\Phi_2(x)\Phi_2'(x)$. At this point, the period of the sequence decreases.

According to Theorem 3, the number of 2-error sequences is 25, the number of 4-error sequences is 25, the number of 10-error sequences is 3125.

According to our computation, in order to make the sum of the odd bits and the sum of the even bits of the original sequence both 0, we randomly select 17^{th} bit of matrix $\mathfrak{A}^{(3)}$ to change. Since the 17^{th} bit of the sequence is odd and bit $42^{nd}(17+25)$ is even, we set 17^{th} bit of the error sequence to 1 and 42^{nd} bit to 2. i.e. $E = 00000\ 00000\ 00000\ 01000\ 00000\ 00000\ 00000\ 00000\ 02000\ 00000$, we can obtain $LC(S+E) = 24$ by the algorithm 1 in [18], $\mathfrak{A}^{(3)}$ remains unchanged and the sum of odd bits and the sum of even bits of the original sequence are both 0. Since the number of 2-error and 4-error sequences is not large, the sequence in the example is a "good" sequence.

In this section, we provide a new method for computing the number of k-error sequences of q-ary sequence with period $2p^2$, While the method is effective, further improvements can be made to enhance its accuracy and efficiency.

Additionally, our approach can be extended beyond q-ary sequences with period $2p^2$ to other periodic binary sequences and q-ary sequences as well. This expansion of our methodology has the potential to broaden its range of applications and impact different areas of research.

5 Conclusion

In this paper, we first analyze the values of the linear complexity of q-ary sequences with period $2p^2$, and study the characteristics of matrices under different linear complexities to compute the corresponding k to obtain the k-error linear complexity of the sequence by four different matrix forms. Then, we analyze all possible k-error sequences in one case and demonstrate the feasibility of applying the matrix method to analyze the number of k-error sequences. And this method can be extended to other periodic binary sequences and q-ary sequences as well.

Acknowledgments

R.Q. Song and Z.H. Niu were partially supported by the State Key Program of National Nature Science Foundation of China (Grant No. 61936001), the National Nature Science Foundation of Shanghai (Grant No. 22ZR1422600) and Key Laboratory of Applied Mathematics of Fujian Province University (Putian University) (NO. SX202102).
C.H. Wu was partially supported by the Natural Science Foundation of Fujian Province (Grant No. 2020J01905), by the Science and Technology Project of Putian City (Grant No. 2021R4001-10). M.X. Chen was partially supported by theby the Science and Technology Project of Putian City (Grant No. 2022SZ3001ptxy05).

References

[1] Z. X. Chen, Z. H. Niu, and C. H. Wu, "On the k-error linear complexity of prime-square periodic binary sequences," *Journal of Cryptologic Research*, vol. 6, no. 5, pp. 574–584, 2019.

[2] T. W. Cusick, C. S. Ding, and A. Renvall, *Stream Ciphers and Number Theory*. Burlington, MA: Elsevier Science, 2004.

[3] C. S. Ding, G. Z. Xiao, and W. J. Shan, *The Stability Theory of Stream Ciphers*. Berlin,Germany: Springer-Verlag, 1991.

[4] R. A. Games and A. H. Chan, "A fast algorithm for determining the complexity of a binary sequence with period 2^n," *IEEE Transactions on Information Theory*, vol. 29, no. 1, pp. 144–146, 1983.

[5] K. Kurosawa, F. Sato, T. Sakata, and W. Kishimoto, "A relationship between linear complexity and k-error linear complexity," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 694–698, 2000.

[6] A. G. B. Lauder and K. G. Paterson, "Computing the error linear complexity spectrum of a binary sequence of period 2^n," *IEEE Transactions on Information Theory*, vol. 49, no. 1, pp. 273–280, 2003.

[7] R. Lidl and H. Niedrreiter, *Finite Fields*. London: Cambridge University Press, 2008.

[8] J. L. Massey, "Shift-register synthesis and bch decoding," *IEEE Transactions on Information Theory*, vol. 15, no. 1, pp. 122–127, 1969.

[9] W. Meidl, "How many bits have to be changed to decrease the linear complexity," *Designs,codes and crytography*, no. 2, p. 33, 2004.

[10] Z. H. Niu, Z. Li, Z.X. Chen, and T.J. Yan, "Computing the k-error linear complexity of q-ary sequences with period $2p^n$," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 95, no. 9, pp. 1637–1641, 2012.

[11] Z. H. Niu, C. Yuan, Z. X. Chen, X. N. Du, and T. Zhang, "On the k-error linear complexity of $2p^2$-periodic binary sequences," *Science China. Information Sciences*, vol. 63, no. 9, 2020.

[12] Ana Sălăgean, "On the computation of the linear complexity and the k-error linear complexity of binary sequences with period a power of two," *IEEE Transactions on Information Theory*, vol. 51, no. 3, pp. 1145–1150, 2005.

[13] M. Stamp and C. F. Martin, "An algorithm for the k-error linear complexity of binary sequences with period 2^n," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1398–1401, 1993.

[14] L. Tan and W. F. QI, "On the k-error sequences of 2^n-periodic binary sequences," *Journal of Electronics and Information Technology*, vol. 30, no. 11, pp. 2592–2595, 2008.

[15] M. Tang and S. X. Zhu, "On the error linear complexity spectrum of p^n -periodic binary sequences," *Applicable Algebra in Engineering Communication and Computing*, vol. 24, no. 6, pp. 497–505, 2013.

[16] S. M. Wei, "An efficient algorithm for determining the k-error linear complexity of binary sequences with periods $2p^n$," *International Journal of Computer Science and Network Security*, vol. 8, pp. 221–224, 01 2008.

[17] S. M. Wei, G. Z. Xiao, and Z. Chen, "A fast algorithm for determining the linear complexity of a binary sequence with period $2^n p^m$," *Science in China Series F*, vol. 44, no. 6, pp. 453–453, 2001.

[18] S. M. Wei, G. Z. Xiao, and Z. Chen, "A fast algorithm for determining the minimal polynomial where of a sequence with period $2p^n$ over $GF(q)$," *IEEE Transactions on Information Theory*, vol. 48, no. 10, pp. 2754–2758, 2002.

[19] C. H. Wu, C. X. Xu, and X. N. Du, "On the k-error linear complexity of q-ary sequence of period p^2," *Journal on Communications*, vol. 40, no. 12, pp. 21–28, 2019.

[20] G. Z. Xiao, S. M. Wei, K. Y. Lam, and et al, "A fast algorithm for determining the linear complexity of a sequence with period p^n over $GF(q)$," *IEEE Transactions on Information Theory*, vol. 46, no. 6, pp. 453–460, 2000.

[21] J. Q. Zhou, "On the k-error linear complexity of sequences with period $2p^n$ over $GF(q)$," *Designs Codes and Cryptography*, vol. 58, no. 3, pp. 279–296, 2010.

Biography

Ruoqi Song was born in 1998 in Shanxi, China. He was received the B.E. degree in Internet of Things Engineering from Harbin Engineering University. He is now studying for a master's degree at the School of Computer Engineering and Science in Shanghai University.

Zhihua Niu was born in 1976 in Shanxi, China. She received the B.S. degree in Mathematics Education from Huaibei Normal University in 1998, and the M.S. degree in Computational Mathematics from Xi'an Jiaotong University in 2002, and the PhD degree in Cryptography from Xidian University in 2005. She is now with the School of Computer Engineering and Science, Shanghai University, China. She worked as a visiting scholar supervised by Prof. Andrew Klapper in University of Kentucky(Lexington) during 2013-2014. Her research interests include pseudo-random sequences, cryptography and information security.

Chenhuang Wu is currently an associate professor of Key Laboratory of Applied Mathematics (Putian University), Fujian Province University, China. He received his M.S. degree in mathematics from Minnan Normal University, China, in 2007. He got his Ph.D degree in Cryptography from the University of Electronic Science and technology of China in 2020. His research interests include stream cipher, elliptic curve cryptography and digital signatures.

Meixiang Chen was born in 1982 in Fujian,China. She received her M.S. degree in mathematics from Fujian Normal University in 2007, and the Ph.D. degree in Representation of Algebra from Fujian Normal University in 2016. She is currently a professor of Key Laboratory of Applied Mathematics(Putian University), Fujian Province University, China. Her research interests include matrix theory and pseudo-random sequences.

A Real Time Food Auto Traceable Authentication System

Chia-Chun Wu[1], Chung-Huei Ling[2], Shyh-Chang Tsaur[2], and Min-Shiang Hwang[2,3]
(Corresponding author: Min-Shiang Hwang)

Department of Industrial Engineering and Management, National Quemoy University[1]
Kinmen County 892, Taiwan
Department of Computer Science and Information Engineering, Asia University[2]
Fintech and Blockchain Research Center, Asia University[3]
Taichung 41354, Taiwan
Email: mshwang@asia.edu.tw

(Received Aug. 15, 2022; Revised and Accepted May 12, 2023; First Online June 25, 2023)

Abstract

The current traceability system certifies traceability accuracy by on-site examination or sampling inspection to promote food safety. However, such an afterward test and trace model no longer guarantees food safety. The food safety scandals that happened in the past few years called into question the effectiveness of the entire examination system. An instantaneous tracking and tracing system will significantly lower the usage of substandard products and low-price substitutes at the marketing stage and prevent dishonest conduct in traceability-related businesses. This study designed a new tracking system incorporating logistic codes and tracking codes to enhance the current agricultural produce's security mechanism and the food traceability certification system. This mechanism adopts the virtual correlation model to reduce certification costs. It provides a complete and sound real-time tracking system for society and the industry to safeguard consumer rights and promote the competitiveness of qualified businesses.

Keywords: Food Traceability System; NFC; QR Code; RFID; Traceability System

1 Introduction

Agricultural produce traceability certification management aims to enhance the quality and safety of processing products and promote people's health and consumer rights. Traceability is defined as the complete records of open and traceable agricultural produce from production, processing, package, distribution to sales, and the labeling are qualified by the certification authority. The distribution process is the transaction affecting the integrity of agricultural products, such as the original package or labeling of agricultural produce, organic agricultural produce, or agricultural processing products. Therefore, complete records could offer correct tracking and tracing for traceability [8].

The agriculture and food traceability system informs consumers about their diet [22, 23]. A consumer can input the "tracking number" of a product certified by the certification authority to acquire information on product areas, producers, production processes (including the use of chemicals and the examination results of Good Agricultural Practice, GAP), output, packaging, and delivering [20]. In this case, the damage coverage and the responsibility belonging can be clarified at the first moment when food safety events occur. It is necessary to manage the tracing source, examine at all levels according to the product removal, recovery, and compensation processes, prevent the events from spreading, and guarantee food safety for consumers [20].

To effectively manage traceability, tracking and tracing, supply, delivery, distribution, and sales information should be thoroughly controlled [9]. Therefore, the traceability system is called Traceability Information, which is eventually achieved by transforming barcode labels into information flow [28]. In addition, the agricultural produce traceability certification management should be satisfied the following "information openness and preservation" and "labeling" requirements:

1) The authority should certify Public information in the information system.

2) Product labeling should cover (1) the label, (2) the name of the product, (3) the trace code, and (4) the way of information openness.

3) The traced, inquired, and open traceability information through the information system should at least contain (1) the name of the product, (2) the name of the agricultural produce businesses, (3) the place of

production, (4) trace code, (5) major event in operation, (6) date of the package, (7) name of certification authority, and (8) validity of the certification.

In short, when any parts of the product label are changed, the changed information needs to be transmitted [5, 12, 19]. The premise is to master all transparent information in and out of the marketing spots. However, it is considered as static records; in fact, the dynamic delivery process is often ignored as it is defined as not changing the label information and no need for printing labels. Therefore, it results in the blind spot of traceability. Accordingly, an accurate automatic traceable tracking and tracing system cannot be established because the tracking and tracing cannot be in active condition. Applying the concept of traceability route to this study, the product delivery at the logistics stage is also included in the tracking and tracing to establish an automatic traceability system [4]. By reinforcing real-time monitoring, it could develop the effectiveness of finding and dealing with problems at the first moment [7].

The successive sections are organized in the following. The tracking and tracing model [11] and the deficiency of the current traceability system are described in Section 2. Section 3 demonstrates the automatic tracking and tracing system model proposed in this study; the tracking and tracing mechanism and the advantages of applying logistics virtual codes are also explained. The differences between the current system and the one in this study are analyzed and compared in Section 4. Finally, conclusions are proposed in Section 5.

2 Tracking and Tracing Model and Deficiency of Current Traceability System

This section explains the tracking and tracing model, coding, and the current traceability system's deficiency.

2.1 Tracking and Tracing Model of Current Traceability System

In the tracking and tracing model of the current traceability system, the information of producers, wholesalers, processing manufacturers, and retailers are transparent, allowing the authorities and the certification authorities to track the product flow and relevant businesses and consumers to trace the product flow. In this case, the tracking and tracing objectives could be achieved with complete records [13]. As a result, tracking products with materials needs to forecast the product flow, and tracing materials from products could check the current source [24]. Finally, a consumer can confirm and prove the product security in the system with the "trace code" on the label. A "trace code" similar to the identity of agricultural produce plays an irreplaceable information flow in the system [9]. The following section will explain how the coding of a "trace code" records the regulated open information and how the system creates a win-win for producers, distributors, consumers, and managers.

2.2 Coding of Trace Code

According to the 2004 coding standards, the trace code was designed based on the structure of the 14-digit traceability trace code (TC) in Table 1 and extended to the distribution code (DC) and electronic distribution code (EC) in Table 2. Furthermore, to cope with the one-print-one-trace code policy of the Agriculture and Food Agency and to complement the inadequacy of the original trace code NNNN, the design is reinforced as an electronic distribution code (EC) in Table 3.

Consistent data exchange standards are used for outputting the column definition and various standards to achieve the food tracking and tracing objectives and complete the food production information system [6, 21, 27]. The product could be upward traced or downward tracked from the shift at stages to label necessary information on the batch of food [14]. Meanwhile, the safety of supply chains can be controlled through production management, logistics process, liability assessment, and risk articulation [14].

2.3 Deficiency of Current Traceability System Coding Model

The food tracking and tracing application management [1, 2,10,21] loads the product information to the tracking and tracing system (Table 4). In addition, it plans a complete food cloud core structure to integrate upstream and downstream businesses in the food industry. Furthermore, it advises businesses on developing the food tracing information system, which expects to expose the flow of problematic products, allow the co-supervision of consumers, and guard the national health and welfare [20].

In Table 4, the overlapped management items in the product differentiation are the critical tracking and tracing information in the system [19]. Nevertheless, because of the shift in product differentiation, it is considered insufficient to master logistics businesses [15].

It is evident that the Delivery barcode in Step 2 conveys the Material barcode in Step 1, and the Delivery barcode in Step 8 conveys the Certification barcode in Step 7 [9]. According to the description in the previous section, the distribution code or the electronic distribution record number in the delivery barcode is the same no matter which logistics delivers the product [21]. The system does not identify or certify it because the logistics delivery process is regarded as internal auditing and tracking [3]. For this reason, a person could duplicate the delivery barcode, and the abnormal situation of two products with one code in the allowed time might appear to result in a loophole. On the other hand, the trace code is updated merely when the content is changed. Therefore, the distribution barcode at the logistics stage will

Table 1: Design of traceability trace code

Format	D	○○○○○	YY	BB	NNNN
Meaning	Category code	Organization code	Year code	Phase code	Serial code
Description	1-2 Agricultural produce 3 Ornamental flower 4 Aquatic product 5 Poultry product 6 Pig 7 Other livestock product 8 (Processing food) 9 (Reserved) 0 Circulation code use	Serial number in TAFT database for production units or manufacturers	20YY	1. Use for mixed product delivery, BB = 00 2. Standing for the BB phase production in the year 3. Use for inadequate digit of serial numbers	Serial number of the batch production given by the information system

Table 2: Design of distribution code

Format	0	0	D	○○○○○	Y	NNNNN
Meaning	Category code			Organization code	Year code	Serial code
Description	Distribution code	Processing code	1-2 Agricultural produce 3 Ornamental flower 4 Aquatic product 5 Poultry product 6 Pig 7 Other livestock product 8 (Processing food) 9 (Reserved) 0 (Reserved)	Serial numbers of production units or manufacturers in TAFT database	200Y	Serial number of the batch production given by the information system

Table 3: Design of electronic distribution code

Format	0	2	D	○○○○○	Y	NNNNN
Meaning	Category code			Organization code	Year code	Serial code
Description	Distribution code	Electronic distribution record number	1-2 Agricultural produce 3 Ornamental flower 4 Aquatic product 5 Poultry product 6 Pig 7 Other livestock product 8 (Processing food) 9 (Reserved) 0 (Reserved)	Serial numbers of production units or manufacturers in TAFT database	200Y	Serial number of the batch production given by the information system

Table 4: Regulations of Food Tracking and Tracing System Management

Number of article			Article 4	Article 5	Article 6
Product differentiation			Manufacturing, processing, formulating	Input	Sales, output
Type of information	Order	Management item			
Supplier	1	Basic information of a business or a company name	✔	✔	✔
	2	Name of product	✔	✔	✔
	3	Net weight, volume, quantity, or measurement	✔	✔	✔
	4	Batch number	✔	✔	✔
	5	Expired date or production date	✔	✔	✔
	6	Date of receiving	✔	✔	✔
	7	Information of raw materials and place (origin) of production	✔	✔	✔
Product flow	1	Basic information of logistics businesses and downstream manufacturers	✔	✔	✔
	2	Name of product	✔	✔	✔
	3	Net weight, volume, quantity, or measurement	✔	✔	✔
	4	Batch number	✔	✔	✔
	5	Expired date or production date	✔	✔	✔
	6	Date of delivery	✔	✔	✔

not need to update the code. In this case, a person will have enough time for fraud to cause a blind spot in tracking and tracing [9]. This is the problem and blind spot this study intends to solve. An automatic tracking and tracing management mechanism combined with the current system is proposed in this study to overcome such blind spots and problems.

3 Automatic Tracking and Tracing Traceability System

An automatic real-time traceable certification tracking and tracing system is named in this study [4]. The system is aware of the product location anytime once the first barcode label is output to the sales and a consumer [2]. Under the safety premise of repetition as fraud, the system immediately alerts any repeated labels to guarantee the management. Furthermore, the traceability route and logistics virtual codes are classified for reinforcing physical codes' tracking and tracing mechanism [4].

3.1 Traceability Tracking and Tracing Mechanism

For a system, the upward tracing-and-inquiring and the downward tracking-and-monitoring are technically both sides when the loaded information is adequate [7]. Besides, abnormity will be tracked so that unpreventable abnormal events can be traced to the sources to explore the causes [14]. For this reason, the operation model for the tracking and tracing mechanism is set before proposing the automatic traceable tracking and tracing system in this study, shown in Figure 1, to construct the proposed traceability [11]. First, the tracking and tracing routes are executed through the system association diagram.

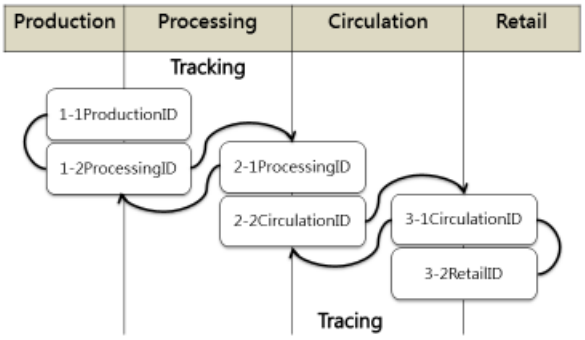


Figure 1: Traceable tracking and tracing multi-level association mechanisms

In Figure 1, at least three association diagrams, (1-1.1-2), (2-1.2-2), and (3-1.3-2), are required for the four traceability stages. For example, the tracking route shows 1-1 production ID→1-2 processing ID→2-1 processing ID→2-2 distribution ID→3-1 distribution ID→3-2 sales ID, and the tracing route reveals the reverse 3-2 sales ID→3-1 dis-

tribution ID→2-2 distribution ID→2-1 processing ID→1-2 processing ID→1-1 production ID. As long as the parts are linked, the required traceability information can be immediately inquired with a product trace code (ID). Under such a mechanism, logistics (ID) virtual codes could reinforce the tracking and tracing mechanism of physical codes [18], allowing products to be tracked and traced anytime.

3.2 Logistics Virtual Code Information Flow Tracking and Tracing Mechanism

In the food and relative product tracking and tracing system, the product flow is regarded as the primary information, stressing "forecasting" the product flow [17] (logistics businesses and downstream manufacturers). This study aims to reinforce the tracking and tracing mechanism of physical codes that should still be followed. To achieve strict tracking and tracing and externalize internal auditing information at the logistics stage, the added trace code is called a "logistics virtual code." Figure 2 shows the logistics virtual code information flow tracking and tracing mechanism proposed in this study.

The delivery process in the logistics business is included in the internal auditing process in current traceability. Concerning the current development of supply chain tracking technology in logistics businesses, it looks reliable to link an external tracing mechanism with the internal tracking system [24–26] when abnormal events occur. However, fraud in the delivery process or the abnormal certification at the delivery destination cannot timely make up for the deficiency. Accordingly, this study proposes combining delivery receipts of a logistics business with the tracking system in a certification center to avoid the risk in the product delivery process. Before a logistics business delivers the product, the product flow has to be accounted for according to the regulations. The traceability is scanned or sensed with a mobile device at the delivery stage for real-time uploading to the traceability certification center and to record individual product traceability, product flow, and mobile device ID. This is the logistics ID, as shown in Figure 2.

Under the structure, the connection of logistics codes, and traceability, it could achieve the advantages of externalization, virtualization, and automation.

3.2.1 Externalization

Because of the boom of logistics supply chains matching with relatively automated logistics devices, the product flow delivered from the logistics to the destination is the standard logistics tracking process of internal auditing in a logistics business [15]. As a result, a logistics business could offer real-time product inquiry services for clients. The processes of making orders, delivery, arrival, and inspection of goods could be achieved through internal tracking. The current traceability system also regards the operation as an external supporting system, but merely auditing risks with sampling inspection and examination [21]. From 1-3 and 2-3, Logistics ID designed at the processing and distribution stages in Figure 2, a logistics business could advise the flow location of an individual product at a time point in the channel. Consequently, it results from externalizing internal operations in a logistics business. When internalizing it in the traceability process is the deserved service of the consumers of a logistics business, the traceability certification unit could understand any product flow with such a design, and the change of externalizing the logistics process to the traceability internalization will have the system integration to develop the effectiveness of complete monitoring.

3.2.2 Virtualization

It is assumed that this designed mechanism is operated under the original traceability coding to promote the system with minimal changes at various stages. Furthermore, under the premise of the traceability code not being updated when the traceability content is changed, the combined logistics ID is regarded as a virtual code for the system's regular operation. From the mechanism in Figure 2, the tracing route does not contain the combined logistics ID. In other words, a logistics ID merely appears in the tracking route and is disposed of after use. Once the product arrives at the designated product flow location, the system will automatically delete the tracking association and recover the association with the original system. Since the logistics ID is not listed in the traceability code, the issuing party does not need to print the logistics ID. Therefore, It presents a virtual state, assists the system in the tracking ability, and applies the current advantages of logistics businesses to enhance the integrity of traceability systems.

3.2.3 Automation

As the above descriptions of externalization and virtualization, this study can be further applied and developed after integrating traceability with the system of a logistics business [15]. For example, the certification center could assign the product flow party and inquire about the product in the traceability tracking and tracing system after receiving the product flow and the logistics ID uploaded by the logistics business. Two auditing points could be mastered in the process; one is the logistics delivery device, and another is the stock system at the product flow end. When the traceability code is scanned or sensed at the first auditing point, the system synchronously starts 1-3 or 2-3 Association in Figure 2 Logistics ID, automatically transmits the logistics ID and the product traceability information of the seller to the buyer, as well as strictly monitors the period for product delivery according to the regulated delivery time management items. When the second auditing point receives the product, the stock system would immediately uploads the product traceabil-

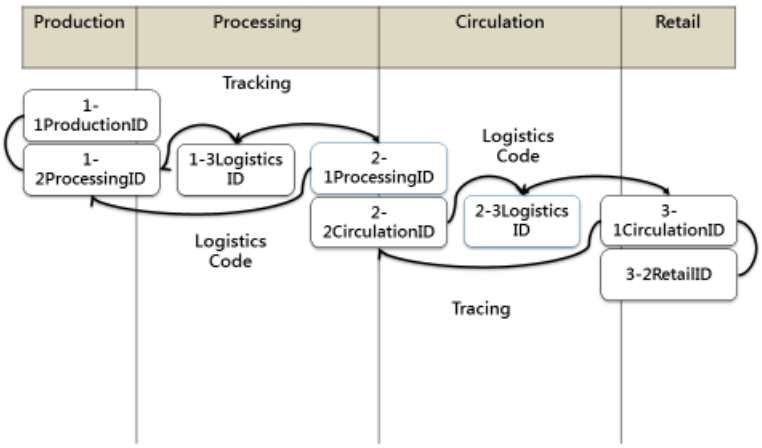


Figure 2: Logistics virtual code information flow tracking and tracing mechanisms

ity to the certification center after scanning or sensing the product traceability to remove the virtual state of a logistics ID. The certification center would calculate the delivery time for standard delivery to the product flow end. If not, the system would immediately trigger the alert message for purposive examination. In this case, the automation process could delete any abnormities induced at the stage to perfect the traceability system and achieve preventive effectiveness.

In sum, the combination of the tracking and tracing mechanism of logistics characteristics proposed in this study presents the advantages of externalization, virtualization, and automation. The system properties are further analyzed and compared to understand the contribution of this study to the current traceability tracking and tracing mechanism.

4 Analysis and Comparison

The comparison between this system model and the current traceability system is demonstrated in Table 5.

4.1 Traceability Coding

A trace code is defined as the code to identify the traceability of agricultural produce of different batches. The design in this study follows the original traceability coding and structures on the original system. However, it is still compatible with another self-designed coding, presenting more excellent expandability by accepting tiny system changes and being compatible with other heterogeneous systems.

4.2 Information Flow Association

As the comparison between Figure 1 and Figure 2, the information flow of the current system shows 1-1 production ID←→1-2 processing ID←→2-1 processing ID←→2-2 distribution ID←→3-1 distribution ID←→3-2 sales ID, where ←→ stands for the tracking route and the tracing route being the same but opposite. The system's information flow in this study divides the tracking and tracing routes into two different routes. The tracing route is consistent with the current system as 3-2 sales ID→3-1 distribution ID→2-2 distribution ID→2-1 processing ID→1-2 processing ID→1-1 production ID, while the tracking route is added the logistics time flow as 1-1 production ID→1-2 processing ID→(1-3logisticsID)→2-1 processing ID→2-2 distribution ID→(2-3logisticsID)→3-1 distribution ID→3-2 sales ID. The tracking route is still the same as the current system after completing the logistics delivery and inspection of goods.

4.3 System Integration

In the era when Cloud is prevalent, internal auditing depends on the operation of a private Cloud, while external auditing relies on constructing a public Cloud. When a producer cannot construct a private Cloud, it is requested by the authority to register relevant production information with excellent agricultural produce certification management and regarding farmers as the internal customers [2]. Therefore, the information at this certification stage could be the indirect internal auditing management measure to construct further the basis of the tracking and tracing traceability system, similar to sharing private Cloud on public Cloud. The logistics virtual code information flow tracking and tracing mechanism designed in this study attempts to externalize the information in the internal auditing private cloud at the logistics stage and includes the traceability in the public Cloud. By applying logistics tracking advantages, it reinforces the tracking and tracing channels of the original system through system integration. As a result, a more efficient tracking and tracing traceability system will be naturally constructed when matching with the relevant law amendment.

Table 5: Comparison between this system and current traceability tracking and tracing mechanism

Differentiation Differentiation	Current tracking and tracing mechanism	Tracking and tracing mechanism in this study
Traceability coding	According to regulations	Following and compatible with current regulations
Information flow association	Traceability stage	Traceability stage and logistics information
System integration	Original traceability system	Combining with the deliver in logistics system
Logistics device ID	Not included	Including virtual code
Automation	Yes	No
Dynamic tracking	No	Yes
Tracking schedule	Discontinuous	Fully
Real-time certification ability	No	Yes
Certification cost	High	Low

4.4 Logistics Device ID

Logistics devices generally can scan or sense barcodes and aim to control the logistics delivery process timely. However, since the current system focuses on distribution information to master the retail and wholesale of products, the logistics device ID has not been included in the tracking and tracing mechanism. This study's design emphasizes complementing the monitoring during the product delivery to block someone from duplicating the traceability barcode. For this reason, logistics' delivery, distribution, and transit storage information is included in the tracking and tracing. Furthermore, the virtual code association, automatically deleted when the product arrives at the assigned product flow location, is applied to densely connect the data. Therefore, the advantages of logistics supply chains could be applied to current traceability for success.

4.5 Automation

As the current system focuses on distribution, the tracking will eventually be entrusted to the internal auditing of logistics which can hardly achieve the efficiency of automation. Therefore, logistics tracking is introduced in this design. Section 3.2.3 mentions that two auditing points derived in the process are utilized for directly uploading the movement of the certification center through current logistics devices and the scanned and sensed traceability of stock to achieve the efficiency of automation.

4.6 Dynamic Tracking

The upstream and downstream relation of the tracking traceability in the current system is undoubted. Regarding the current system, there are correspondent recording standards for production, processing, and distribution for system tracking. However, they are point tracking, after all. Therefore, the shifting information between points at each stage is still not included in the system information flow. Therefore, dynamic tracking can hardly be operated. Besides, the start of tracking is merely established on an artificial examination, so it could not satisfy the initiative. Nonetheless, the technique introduced to the design in this study is based on dynamic tracking, so the certification unit could immediately construct complete tracking information when receiving the logistics code and the product traceability label, making the certification mechanism automatically compared with the product flow and the delivery time to acquire the dynamic tracking effect.

4.7 Tracking Schedule

The product flow schedule is often changed because of delivery locations. When a speculator delivers an imitation (the real one is purposively delayed), it takes 8 hours for the repetition collision (the arrival), as the situation in Taiwan. As the delivery at the logistics stage is interrupted, the current system cannot inquire about the collision during the delivery, and it has to wait until the sales stage. Therefore, the tracking time is comparatively more extended than the design in this study; particularly, the logistics code is compared with the product flow information and the delivery time in this study, so the delivery problem with an imitation could be blocked. Consequently, when purchasing in a correspondent certification department, a consumer can reduce the risk in food safety to zero. It is thanks to the design of seamless tracking time.

4.8 Real-time Certification Ability

The so-called real-time certification refers to the ability to inspect illegal traceability products in real-time. The current system focuses on the change of product content to decide the update of the traceability barcode [16]. Therefore, the certification works depending on the sampling inspection result. Even though a problematic product is inspected, it can hardly reconstruct consumers' confidence once the damage occurs. Therefore, the importance of real-time certification for the system is apparent. The

design in this study especially takes the product certification at the delivery stage into account to make up for the deficiency of the current system. The product collision or irrational delivery time could be discovered and handled with the assistance of logistics virtual codes to complement and improve the current system, and it is a design system with high practicability.

4.9 Certification Cost

The certification cost of the current system is based on the workforce, and the certification performance requires a sufficient organizational system. It is considered outdated in the current food cloud era [28]. This design externalizes the internal delivery in the private logistics cloud to the internal parts of traceability with an automated tracking system equipment in the current logistics system. The certification unit merely needs to certify the devices of a logistics business. It is included in the tracking mechanism to obtain timely, dynamic, and time-reducing effectiveness, reducing the certification cost and dramatically enhancing the certification performance. This design could reduce the authority's certification cost by promoting the traceability 2.0 policy.

5 Conclusion

To overcome the blind spot and problem in certification management during food delivery, the automatic traceable system proposed in this study covers the internal auditing of logistics delivery in the traceable internal auditing tracking mechanism. It applies the virtual association model to delete it after the product completes the assigned product flow and is thoroughly examined. Therefore, it could complement the current system's deficiency and enhance the system's real-time tracking and certification functions. From the analysis and comparison, the logistics device ID is included in this study through the system integration with logistics information without changing the original traceable coding structure. Therefore, it presents the efficacy of automation, dynamic tracking, and reduction of tracking schedules compared to the current system. Besides, the unique real-time certification ability essentially reduces the certification cost that presents high practicability. Therefore, this design is expected to assist the authority in promoting the traceability 2.0 policy, meeting the new traceability era, maintaining food safety, reconstructing consumer confidence, and enhancing the competitiveness of quality businesses.

Acknowledgments

The Ministry of Science and Technology partially supported this research, Taiwan (ROC), under contract no.: MOST 109-2221-E-468-011-MY3, MOST 108-2410-H-468-023, and MOST 111-2622-8-468-001 -TM1.

References

[1] M. M. Aung, Y. S. Chang, "Traceability in a food supply chain: Safety and quality perspectives", *Food Control*, vol. 39, pp. 172-184, 2014.

[2] Y. Bao, Y. Bao, "Chicken and egg food traceability system based on NFC and QR code technology", in *Proceedings of 12th International Conference on Electronics, Communications and Networks (CECNet'22)*, Frontiers in Artificial Intelligence and Applications, vol. 363, pp. 191-197, 2022.

[3] A. Bechini, M. G. C. A. Cimino, F. Marcelloni, and A. Tomasi, "Patterns and technologies for enabling supply chain traceability through collaborative e-business," *Information and Software Technology*, vol. 50, pp. 342-359, 2008.

[4] P. Bernardi, C. Demartini, F. Gandino, B. Montrucchio, M. Rebaudengo, E. R. Sanchez, "Agri-food traceability management using a RFID system with privacy protection," in *21st International Conference on Advanced Networking and Applications (AINA '07)*, pp. 68-75, 2007.

[5] Y. C. Chen, W. L. Wang, M. S. Hwang, "RFID authentication protocol for anti-counterfeiting and privacy protection", in *The 9th International Conference on Advanced Communication Technology*, pp. 255–259, 2007.

[6] Y. C. Chen, W. L. Wang, M. S. Hwang, "Low-cost RFID authentication protocol for anti-counterfeiting and privacy protection", Asian Journal of Health and Information Sciences, vol. 1, no. 2, pp. 189-203, 2006.

[7] M. G. C. A. Cimino, B. Lazzerini, F. Marcelloni, and A. C. Tomasi, "Cerere: An information system supporting traceability in the food supply chain", in *Seventh IEEE International Conference on E-Commerce Technology Workshops*, pp. 90-98, 2005.

[8] S. Dey, S. Saha, A. K. Singh, K. McDonald-Maier, "FoodSQRBlock: Digitizing food production and the supply chain with blockchain and QR code in the cloud," *Sustainability*, vol. 13, 2021.

[9] L. Dong, P. Jiang, F. Xu, "Impact of traceability technology adoption in food supply chain networks", *Management Science*, vol. 69, no. 3, pp. 1518-1535, 2023.

[10] N. Faisal, F. Talib, "Implementing traceability in Indian food-supply chains: An interpretive structural modeling approach", *Journal of Foodservice Business Research*, vol. 19, no. 2, pp. 171-196, 2016.

[11] D. Folinas, I. Manikas, B. Manos, "Traceability data management for food chains," *British Food Journal*, vol. 108, no. 8, pp. 622-633, 2006.

[12] M. S. Hwang, C. H. Wei, C. Y. Lee, "Privacy and security requirements for RFID applications", *Journal of Computers*, vol. 20, no. 3, pp. 55–60, Oct. 2009.

[13] Y. M. Hwang, J. Moon, S. Yoo, "Developing a RFID-based food traceability system in Korea ginseng industry: Focused on the business process reengineer," *International Journal of Control and Automation*, vol. 8, no. 4, pp. 397-406, 2015.

[14] Q. Huang, "On establishment of food traceability system with internet of things", in *Proceedings of the 12th International Conference on Computer Engineering and Networks (CENet'22)*, Lecture Notes in Electrical Engineering, vol. 961, pp. 23-28, 2022.
[15] C. Y. Liu, *RFID and EPC Network Operation Models for A Multi-Stage and Multi-Level Supply Chain*, Master Thesis, National Tsing Hua University, 2006.
[16] M. Mattevi, J. A Jones, "Food supply chain: Are UK SMEs aware of concept, drivers, benefits and barriers, and frameworks of traceability?" *British Food Journal*, vol. 118, no. 5, pp. 1107-1128 , 2016.
[17] T. A. McMeekin, J. Baranyi, J. Bowman, P. Dalgaard, M. Kirk, T. Ross, S. Schmid, M. H. Zwietering, "Information systems in food safety management", *International Journal of food Microbiology*, vol. 112, pp. 181-194, 2006.
[18] S. Piramuthu, W. Zhou, *RFID and Sensor Network Automation in the Food Industry: Ensuring Quality and Safety through Supply Chain Visibility*, Wiley, 2016.
[19] J. Qiao, M. Hao, M. Guo, "Design of meat product safety information chain traceability system based on UHF RFID", *Sensors*, vol. 23, no. 7, p. 3372, 2023.
[20] P. Saranya, R. Maheswari, "Proof of transaction (PoTx) based traceability system for an agriculture supply chain", *IEEE Access*, vol. 11, pp. 10623-10638, 2023.
[21] C. Song, Z. Wu, J. Gray, Z. Meng, "An RFID-powered multi-sensing fusion industrial iot system for food quality assessment and sensing", *IEEE Transactions on Industrial Informatics*, pp. 1-11, 2023. doi: 10.1109/TII.2023.3262197
[22] E. S. T. Wang, H. C. Lin, M. C. Tsai, "Effect of institutional trust on consumers' health and safety perceptions and repurchase intention for traceable fresh food," *Foods*, vol. 10, 2021.
[23] L. Wang, Y. He, Z. Wu, "Design of a blockchain-enabled traceability system framework for food supply chains," *Foods*, vol. 11, 2022.
[24] C. H. Wei, M. S. Hwang, Augustin Y. H. Chin, "A secure privacy and authentication protocol for passive RFID tags," *International Journal of Mobile Communications*, vol. 15, no. 3, pp. 266–277, 2017.
[25] C. H. Wei, M. S. Hwang, Augustin Y. H. Chin, "An authentication protocol for low-cost RFID tags", *International Journal of Mobile Communications*, vol. 9, no. 2, pp. 208–223, 2011.
[26] C. H. Wei, M. S. Hwang, Augustin Y. H. Chin, "An improved authentication protocol for mobile agent device in RFID," *International Journal of Mobile Communications*, vol. 10, no. 5, pp. 508–520, 2012.
[27] C. H. Wei, M. S. Hwang, Augustin Y. H. Chin, "Security analysis of an enhanced mobile agent device for RFID privacy protection," *IETE Technical Review*, vol. 32, no. 3, pp. 183–187, 2015.
[28] X. Zhou, Q. Zhu, Z. Xu, "The role of contractual and relational governance for the success of digital traceability: Evidence from Chinese food producers", *International Journal of Production Economics*, vol. 255, p. 108659, 2023.

Biography

Chia-Chun Wu received a Ph.D. degree from the Department of Computer Science and Engineering, National Chung-Hsing University, Taichung, Taiwan, in 2011. He is currently an associate professor at the Department of Industrial Engineering and Management, National Quemoy University, Kinmen County, Taiwan. His current research interests include artificial intelligence, internet of things (IoT), database security, secret image sharing, mobile applications development, and digital image techniques.

Chung-Huei Ling received Ph.D. degree from Computer Science and Information Engineering Department of Asia University (Taiwan) in 2016, and M.S. in Applied computer science and technology from Azusa Pacific University, Azusa, California, USA in 1990 and M.B.A in accounting from Northrop University, Los Angeles, California, USA in 1989. His research interests include information security, cloud computing, and radio frequency identification.

Shyh-Chang Tsaur received the B.S. in Electronic Engineering from National Taiwan University, Taiwan, in 1967; the M.A. in Physics from State University of New York at Stony Brook, USA, in1969; the Ph.D. in Electronic Engineering from Carnegie Mellon University, USA, in 1973. Dr. Tsaur with Dr. C Kuo jointly have received more than 10 US patents in Semiconductor Memories during his work in Texas Instruments, USA from 1973 to 1981. From 1981 to 1996, Dr. Tsaur has been in computer industries for 15 years including owning a PC store, employed as CIO in CMS, CA, USA, Information consultants, etc. Since 1996, Dr Tsaur has been employed as the Special Assistant to HCG Chairman for 5 years successfully to reengineer MIS department; hired as an information consultant of TSANN KUEN 3C Group to accomplish a real time EIS system of 150 chain stores in one year; a professor in CSIE department of Asia University until he retired. In last ten years, in addition to teaching in Universities, Dr. Tsaur has co-authored 3 books: RFID principle, Application and Implementation; Database System Theory and Applications; Cloud Computing Introduction: Entering APP Software World.

Min-Shiang Hwang received M.S. in industrial engineering from National Tsing Hua University, Taiwan in 1988, and a Ph.D. degree in computer and information science from National Chiao Tung University, Taiwan, in 1995. He was a distinguished professor and Chairman of the Department of Management Information Systems, National Chung Hsing University, during 2003-2011. He obtained 1997, 1998, 1999, 2000, and 2001 Excellent Research Awards from the National Science Council (Taiwan). Dr. Hwang was a dean of the College of Computer

Science, Asia University (AU), Taichung, Taiwan. He is currently a chair professor with the Department of Computer Science and Information Engineering, AU. His current research interests include information security, electronic commerce, database, data security, cryptography, image compression, and mobile computing. Dr. Hwang has published over 300+ articles on the above research fields in international journals.

A Non-injected Traffic Backdoor Attack on Deep Neural Network

Jiahui Wang, Jie Yang, Binhao Ma, Dejun Wang, and Bo Meng
(Corresponding author: Bo Meng)

School of Computer Science, South-Central Minzu University
Wuhan 430074, China
Email: mengscuec@gmail.com

(Received Nov. 28, 2022; Revised and Accepted May 12, 2023; First Online June 25, 2023)

Abstract

Deep neural networks are highly vulnerable to data poisoning attacks, adversarial sample attacks, backdoor attacks, and other attacks. Most backdoor attacks are against image identification and natural language processing. Still, they pay little attention to the backdoor attack using data traffic in deep neural networks, which can break deep learning-based intrusion detection systems. Hence, firstly, we propose a non-injection traffic backdoor attack on deep neural networks in intrusion detection systems, capable of misleading DBN and LeNet-5 detection data and classifying attack traffic as normal network behavior during detection. After that, we analyze dataset CSE-CIC-IDS2018, find three problems, and optimize it by data cleaning, de-duplication, standardization, and feature coding. Finally, we evaluate the proposed traffic backdoor attack using the optimized dataset CSE-CIC-IDS2018; When the victim network is DBN, the proposed NITBA outperforms DeepFool and C&W by 15.94% and 28.94%in ASR, respectively, and GTAS takes only 3.1s. When the victim network is LeNet-5, the proposed NITBA outperforms DeepFool and C&W in ASR by 11.55% and 23.52%, and GTAS takes only 5.7s.

Keywords: Backdoor Attack; DBN; Deep Neural Network; Traffic Attack

1 Introduction

Deep neural network (DNN) in Deep learning has been a great success in many applications in the last few years, such as voice recognition [1], image processing [2], and face recognition [3, 4]. However, the security attacks on DNN have also aroused widespread concern, just like backdoor attacks [5], adversarial attacks [6, 7], and data-poisoned attacks [8,9], among which backdoor attacks are more flexible, stealthy, and sophisticated. Specifically, backdoor attacks can affect all phases of the machine-learning pipeline.

More and more backdoor attacks against image identification and natural language processing are emerging today. Guo *et al.* [10]proposed a simple backdoor attack for face-matching systems called the generic identity attack; Turner *et al.* [11] proposed to perturb the pixel value of a benign image with the backdoor trigger amplitude instead of replacing the corresponding pixel with the selected mode. For attacking a large number of recently active pre-trained models in natural language processing, Kurita *et al.* [12]used specific keywords as triggers to poison the model weights for backdoor attacks; Chen *et al.* [13] further generalized backdoor attacks by dividing the triggering mechanism into three levels and showing that a successful trigger should not change the normal tags of the original sentence but mislead the model to classify it as the target tag.

Few researchers have focused on backdoor attacks using data traffic in deep neural networks, which can break deep learning-based intrusion detection systems. Hence, we propose a Non-injected Traffic backdoor attack on a Deep neural network called NITBA. Our work is summarized below:

1) Design a new backdoor attack called NITBA, which generates aggressive data traffic as a trigger to attack without injection training. The model includes a generation module, a converter module, and a detection module. The generation module takes a generative adversarial network model to generate data, the converter module contains a random forest algorithm and a converter that combines data, and the detection module is a deep belief network-based model for intrusion detection systems and convolutional neural networks LeNet-5.

2) Analyze dataset CSE-CIC-IDS2018 and find three problems and optimize it to meet the requirements of the experiment by data cleaning, de-duplication, standardization, and feature coding.

3) ASR and GTAS are applied as evaluation metrics for the proposed NITBA. When the victim network

is DBN, the proposed NITBA outperforms DeepFool [14] and C&W [15] by 15.94% and 28.94%in ASR, respectively, and GTAS takes only 3.1s. When the victim network is LeNet-5, the proposed NITBA outperforms DeepFool and C&W in ASR by 11.55% and 23.52%, and GTAS takes only 5.7s, using the optimized dataset CSE-CIC-IDS2018.

2 Related Work

The backdoor attack is a classic topic in the field of system security. Backdoor attacks were first proposed for image data, so most backdoor attacks are studied in computer vision. Gu *et al.* [5] first introduced this problem into the depth model by poisoning some training samples. This method is called BadNets. BadNets is the representative of visible attacks, opening the era of this field. Almost all subsequent poisoning-based attacks are based on this method. Guo *et al.* [10]proposed a simple backdoor attack for face-matching systems, called the generic identity attack, which can use a particular face to impersonate an arbitrary legitimate face class. The authors modified the normal data by replacing one of the two face data with a specific face as the pattern for activating the backdoor, changing the label to legitimate, and then training the network using the poisoned dataset. In [11], Turner *et al.* proposed to perturb the pixel value of a benign image with the backdoor trigger amplitude instead of replacing the corresponding pixel with the selected mode.

Most backdoor attacks assume that backdoor triggers are independent of benign images. Therefore, attackers need to modify images in digital space to activate hidden backdoors during reasoning. Agdasaryan *et al.* first discussed this problem and proposed a new type of backdoor attack [16,17], the so-called backdoor attack. Specifically, they proved that assigning the tags selected by attackers to all images with specific features (such as green cars or cars with racing stripes) for training can create semantic backdoors in the infected DNN.

With the introduction of a series of backdoor attack schemes against DNN, corresponding defense schemes have also emerged. Different deep learning technologies are implemented in network intrusion detection to detect malicious intrusion [18]. Existing mainstream backdoor attack defense mechanisms can be divided into detection, input mitigation, and model mitigation approaches.

The detection-based approach aims at detecting malicious training samples by analyzing the model behavior. For example, Chen *et al.* [19] propose activation values in the latent space, and Gao *et al.* [20] propose detecting potential backdoors by predicting disturbed images.

The input mitigation method attempts to remove the input trigger by changing or filtering the image so that even if the model is injected with a backdoor (i.e., the backdoor will not be activated), the model still usually works. Li *et al.* [21] proposed a transformation-based defense approach that alters an entire image by some transformation (e. g. flipping or scaling).

In contrast to the above approach for deploying models, the model mitigation approach aims to mitigate the threat of backdoor attacks before deployment. For example, Wang *et al.* [22] detect whether the trained model has been injected into the back door by searching for possible trigger patches.

3 Preliminaies

3.1 DNN

Deep Neural Network (DNN) [23]is a multilayer unsupervised neural network. It uses the upper layer's output features as the next layer's input for feature learning. After layer-by-layer feature mapping, it maps the features of the existing spatial samples to another feature space to learn to have better feature expressions for the current input. The depth neural network has many nonlinear mapping feature transformations, which can fit highly complex functions.

The deep neural network model is a multilayer perceptron (MLP). The principle of the perceptron is to find the most reasonable and robust hyperplane among categories. The most representative perceptron is the support vector machine (SVM) algorithm. The deep neural network includes an input, output, and hidden layer. Like perceptron, it still uses hyperplane to extract the features of sample data. As introduced in SVM and logical regression, perceptron can realize linear separability after raising the dimensions of sample data through kernel function. The algorithm to find the boundaries and planes of various categories of data is also called the discriminant algorithm. The essence of a discriminant algorithm is to use conditional probability to get the classification boundaries; Another kind of algorithm is called generative, which uses joint probability to complete data classification. Typical generative algorithms include Hidden Markov Model, Naive Bayes, etc.

3.2 WGAN-GP

The disappearance of gradients in the traditional Generative Adversarial Networks (GAN) model training process is that the Jensen-Shannon (JS) divergence or Kullback-Leibler (KL) divergence cannot perform gradient updates when the probability distributions do not overlap. Finally, model training cannot be performed. The Wasserstein GAN (WGAN) introduces the mathematical concept of Wasserstein distance and adds a Lipschitz constraint, which can effectively solve the problems existing in the traditional GAN model. Wasserstein distance, also known as Earth-Mover (EM) distance in Equation (1):

$$\mathrm{W}(P_r, P_g) = \inf_{\gamma \sim \pi(P_r, P_g)} \mathrm{E}_{(x,y)\sim\gamma}[||x - y||] \qquad (1)$$

The characteristic of the Wasserstein distance is that even if the two probability distributions do not overlap,

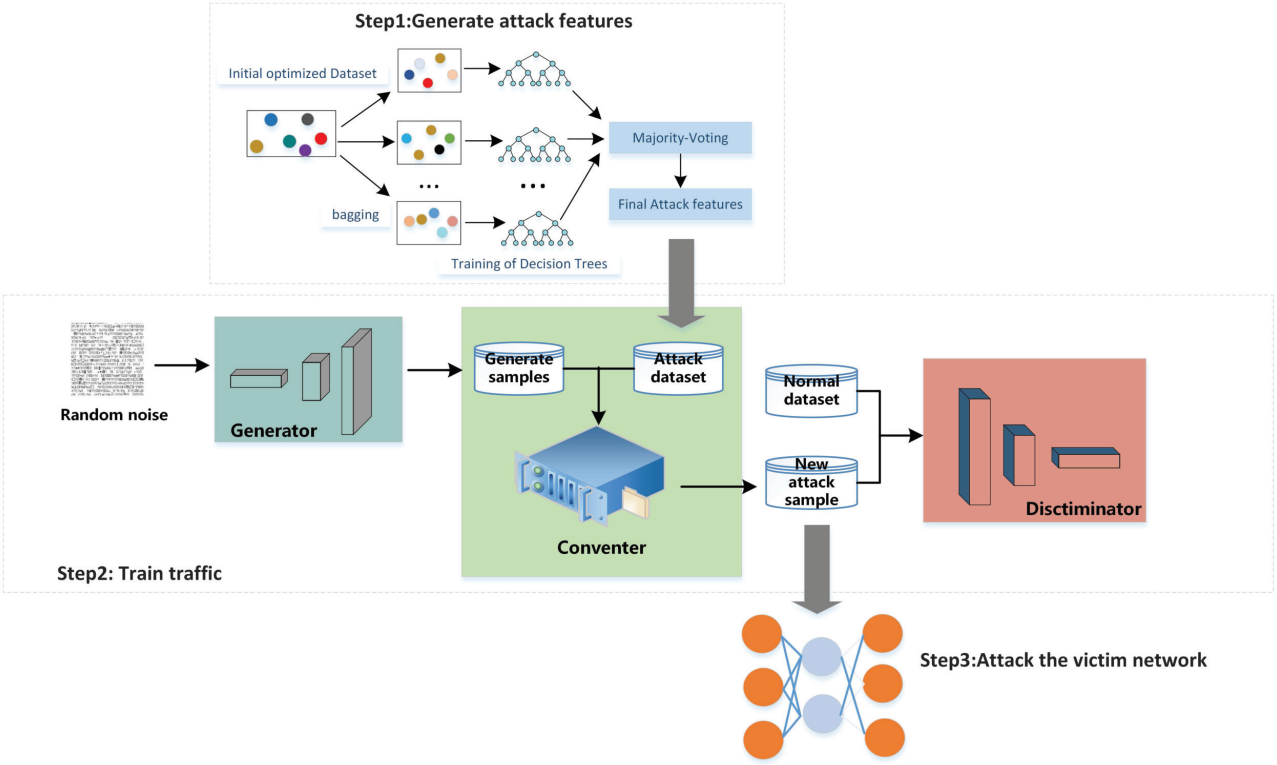


Figure 1: The overall pipeline of Non-injected Traffic backdoor attack on Deep neural network

the Wasserstein distance can still reflect their distance. At the same time, JS and KL divergence are prone to mutation, while the curve of Wasserstein distance is smooth, which can provide stable gradient information for parameter learning. Therefore, the vanishing gradient problem caused by JS divergence or KL divergence does not occur with WGAN. However, related research shows that the training of the WGAN model is prone to gradient explosion. Based on this, some researchers have proposed the concept of gradient penalty to suppress gradient information.

4 Threat Model

Backdoor attacks can occur at any stage of the deep learning process. In this article, we introduced the threat model for our proposed backdoor attack according to the attacker's capabilities and the attacker's goals, as shown below:

The attacker's capabilities: The adversary can get the attacked model and have information about the components. However he can only input data to get the model's output and loss, and not modify any model parameters or the training process.

Attacker's goal: Our goal is to be able to attack deep learning-based intrusion detection systems and reduce their detection rate to generate high-quality attack samples. Precisely, we can fit the feature distribution of normal network behavior data. We can wrap the generated attack samples into the normal network data detected by the victim network to conduct backdoor attacks successfully.

5 Overview

The backdoor attack NITBA we proposed consists of three key steps: generate attack features, train traffic, and attack the victim network. The overall pipeline is shown in Figure 1.

Step 1: Generate attack features
We use the random forest algorithm to train and learn the preprocessed dataset to obtain the ranking of the data features. A random forest is a combination of Bagging and decision trees. The initial data set is extracted by bootstrapping to receive a training set, and multiple extractions are performed to construct multiple training subsets. Each training subset is used to train a decision tree model independently, and these decision trees are randomized in terms of a training set selection and feature selection. The final classification result is determined using all the decision tree votes. Finally, we select the features with higher scores as attack features with attack capability and the rest as non-attack features.

Step 2: Train traffic
We use the WGAN-GP network for traffic training, adding a converter in between the generator and the

discriminator. First, the input to the generator is a random noise variable. After a fully connected neural network, sample data is output. This sample data learns the distribution of features of normal traffic samples, which, in principle, do not have the corresponding attack capability. The converter screens the non-attack features in this traffic data sample and combines them with the attack traffic sample's attack features to produce a new attack traffic sample. At this point, the attack sample has different attack capabilities depending on the combined attack features. For example, the attack features of the Distributed Denial of Service (DDoS) attack traffic data are combined into the data sample generated by the generator, which has the attack capability of a DDoS attack.

The discriminator discriminates both the new attack samples and the data traffic samples of normal network behavior. The discriminant result of the attack sample is False (0), and the discriminant result of the normal network behavior data is True (1). And the discriminated results are given to the generator as the basis for the generator to optimize the training basis, and the final training results converge to Nash equilibrium to generate high-quality attack traffic samples as the trigger of this attack.

Step 3: Attack the victim network

Here we choose DBN [24] and LeNet-5 [25] as the victim network model of the experiment. DBN is a typical deep learning algorithm combined with intrusion detection techniques to screen and detect data traffic of attack behavior.

DBN derives various classes depending on the design of the top-level classification algorithm, among which, in the deep belief network based on support vector machine (SVM), i.e., DBN-SVM, the data samples are processed by RBM to achieve data dimensionality reduction. Then the SVM algorithm is used to find the data's optimal decision hyperplane. The detection rate is higher, and the classification is more accurate. So we firstly regard DBN-SVM as the victim network to detect the final attack performance. DBN-SVM trains the optimized dataset and records its detection accuracy.When WGAN-GP network training is stable, the generator and discriminator are close to Nash equilibrium. Input the generated attack samples into the DBN trained with parameters, and evaluate the quality of the attack sample flow generated by the WGAN-GP network through the difference between the detection accuracy before and after.

Meanwhile, convolutional neural network-based network traffic classification methods have been widely applied to various traffic environments. Ahmad *et al.* proposed to use a convolutional neural network as an intrusion detection system for network traffic to distinguish and identify intrusions of network attacks [26]; Mercaldo *et al.* pointed out that grayscale image samples can be obtained from mobile traffic environments [27], so we chose LeNet-5 as another victim model, and his network structure and parameters are shown in Table 1.

Table 1: Network structure of LeNet-5

Name		Size
Input		16×16
C1 Convolutions	Convolution kernel	8×(3×3)
	Output	8×(16×16)
S2 Subsampling	Sampling Window	2×2
	Output	8×(8×8)
C3 Convolutions	Convolution kernel	16×(5×5)
	Output	16×(8×8)
S4 Subsampling	Sampling Window	2×2
	Output	16×(4×4)
C5 Full connection	Convolution kernel	128×(4×4)
	Output	128×1
Output		12×1

6 Implementation and Evaluation

6.1 Implementation Details

Experiment environment

Based on the attack methods, the following experimental environment is set up. The operating system is 64-bit Windows 10, and the CPU used is AMD Ryzen 7 5800H. The development environment is TensorFlow 1.13.0, CUDA10.0, and CuDNN7.4. The learning rate of the generative adversarial network is set to 0.0005, and the learning rate of the deep belief network is set to 0.5.

Metrics

Attack success rate (ASR) and the generation time of attack sample (GTAS) are the performance metrics of NITBA, in which ASR evaluates the effectiveness of backdoor attacks and GTAS evaluates the efficiency. The mathematical formulas of GTAS and ASR are as in Equation (2) and Equation (3):

$$\mathrm{GTAS} = Timestamp\_end - Timestamp\_begin \quad (2)$$

Timestamp_end is the end time of the sample generation, while Timestamp_begin is the start time.

$$ASR = \frac{\mathrm{FP}}{\mathrm{TP} + \mathrm{FP} + \mathrm{FN} + \mathrm{TN}} \quad (3)$$

We judge the metrics of the experimental results with the help of a confusion matrix as an evaluation criterion.The confusion matrix can reflect the classification performance in the second classification task, as Table 2 shown. In this experiment, set the generated attack traffic samples as the positive class, and

Table 2: Confusion Matrix

Confusion Matrix		Predict	
		Positive	Negative
Actual	Positive	TP	FN
	Negative	FP	TN

the normal traffic data samples as the negative class. TP is the number of positive data classified as positive; FN is the number of positive data classified as negative data; FP is the number of negative data classified as positive data; TN is the number of negative data classified as negative; The following table shows the confusion matrix describing the detection results. The accuracy rate is the ratio of the number of samples correctly classified by the classifier to the total number of samples. The classification error rate equivalent to ASR can reflect the probability of misclassification, i.e., the effectiveness of backdoor attacks.

Optimize CSE-CIC-IDS2018 dataset

We select the CSE-CIC-IDS2018 dataset, which is information on data traffic features collected by the Canadian Institute for Cybersecurity by setting up systems that simulate normal network behavior and various network attacks. The dataset contains 25 types of user behaviors set up by the institute to generate normal data flows and 6 types of attack behaviors data flow generated by various network attack tools that are common in reality. All the traffic data were extracted through the CICFlowMeter tool with 80 network traffic features [28, 29]and exported as CSV files. The researchers at the institution set up the complete network infrastructure. They performed attacks based on it. The following six types of attacks are included in this dataset: Bruteforce attack, Botnet, Denial-of-Service, Web Attacks, Infiltration of the network from inside, and Distributed Denial-of-Service. These attack methods are subdivided into various categories depending on the attack tools used, and the dataset is labeled for these categories using data tags. And through the captured data traffic and network logs, 80 data features are extracted on CICFlowMeter-V3, and we can classify the data by learning these features. The attribute features of the dataset are shown in the following Table 3.

After analyzing the CSV file dataset, we find that the CSE-CIC-IDS2018 dataset has the following problems:

1) There are a small amount of null data and infinite value data in the dataset;
2) The normal network behavior data contains a large amount of repeated and redundant data;
3) The data samples are unevenly distributed, with too many normal data samples and too few data samples of Web Attacks, which need to be revised to train the model.

To address these problems, the CSE-CIC-IDS2018 dataset is processed as follows.

1) Remove data samples containing Nan and Inf from the data set.
2) Deduplication, deleting duplicate data samples from the dataset.
3) Data balance. Web Attacks' data samples are less than 1000, accounting for only 0.006%. The amount of data is far lower than that of other attack samples. Therefore, we choose to delete the relevant samples of Web Attacks directly. The new dataset comprises other data samples with the same amount of data. More experimental data sets will easily lead to long model training time and heavy computer hardware equipment burdens. Here, 15000 pieces of data are selected from each data sample to form a data set with a total of 95000 pieces of data as the input of the training model.
4) The data type of the timestamp attribute is date data, which is converted to the number type of the timestamp.
5) The normalization method normalizes all data values except for the Label attribute. The normalization method scales the data values between 0 and 1 to balance the units of measure between different features. The formula is as Equation (4):

$$x^* = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \tag{4}$$

where x^* is the original data.

6) As too few Web attack samples and relevant data are deleted, there are only six categories of tag attributes. A heat code processes the Label dataset, and the following feature representation methods are obtained in Table 4.

6.2 Results and Discussions

Since the backdoor attack we designed is zero-injection, existing backdoor attack methods are required to be injected, which may lead to failure to generate the attack success rate ASR. In contrast, general adversarial attacks are not required to be injected. The probability of generating a success rate will be much higher, so we chose two more typical adversarial attack methods DeepFool and C&W, to conduct the experimental comparison work.

Table 3: Attributes of dataset

Data type	attributes
date	Timestamp
value	Dst Port, Protocol, Flow Duration, Tot Fwd Pkts,TotLen Fwd Pkts,TotLen Bwd Pkts, Pkt Len Min, Fwd Pkt Len Mean, Fwd Pkt Len Std, Bwd Pkt Len Max,Bwd Pkt Len Min,Bwd Pkt Len Mean, Bwd Pkt Len Std,Flow Byts/s,Flow Pkts/s,Flow IAT Mean, Flow IAT Std,Flow IAT Min, Fwd IAT Tot, Fwd IAT Mean, Fwd IAT Std,Fwd IAT Max, Fwd IAT Min,Bwd IAT Mean, Bwd IAT Std, Bwd IAT Max,Bwd IAT Min, Fwd PSH Flags, Bwd PSH Flags,Fwd URG Flags, Bwd URG Flags, Fwd Header Len, Bwd Header Len, Fwd Pkts/s, Bwd Pkts/s,Min, Pkt Len Max, Pkt Len Mean, Pkt Len Std, Pkt Len Var, FIN Flag Cnt, SYN Flag Cnt,PSH Flag Cnt, ACK Flag Cnt, URG Flag Cnt, CWE Flag Count,ECE Flag Cnt, Down/Up Ratio,Fwd Seg Size Avg, Bwd Seg Size Avg, Fwd Byts/b Avg, Fwd Pkts/b Avg, Fwd Blk Rate Avg,Byts/ Bwd Pkts/b Avg, Bwd Blk Rate Avg, Subflow Fwd Pkts,Subflow Fwd Byts,Subflow Bwd Byts, Init Fwd Win Byts, Init Bwd Win Byts, Fwd Act Data Pkts, Fwd Seg Size Min,Active Mean, Active Std, Active Max, Active Min, Idle Mean, Idle Std, Idle Max, Idle Min
string	Label

Table 4: One-Hot Encoder of Lable

Eigenvalues of lable	One-hot encoding
Benign	0 0 0 0 0 1
DDos	0 0 0 0 1 0
Dos	0 0 0 1 0 0
Botnet	0 0 1 0 0 0
Bruteforce	0 1 0 0 0 0
Infiltration	1 0 0 0 0 0

We compare NITBA with the C&W and DeepFool attack against DBN-SVM and LeNet-5 with the optimized dataset to evaluate GTAS and ASR. Apart from that, the results of the initial data attack on the DBN-SVM and LeNet-5 will also be shown. DeepFool adds perturbations to the data variables by the shortest distance between the data variables and the decision hyperplanes of the different categories. Its minimum perturbation variables $r_*(x_0)$ are as in Equation (5):

$$r_*(x_0) = \frac{|f_l(x_0) - f_k(x_0)|}{||w_l(x_0) - w_k(x_0)||_2^2}(w_l(x_0) - w_k(x_0)) \quad (5)$$

wheref_k is the categorical decision hyperplane function to locate the variable, f_l is the closest categorical decision hyperplane for the variable, and w is the gradient information for thecategorical prediction.

C&W attack adds a perturbation to the data sample by setting two value functions to determine the minimum value of the gap between the adversarial sample and the corresponding clean sample and the probability that the adversarial sample should make the model misclassify. In this way, the value function of C&W is defined as in Equation (6):

$$\min_{w_n} ||r_n|| + c \bullet f(\frac{1}{2}(\tanh(w_n) + 1)) \quad (6)$$

where f define as Equation (7):

$$f(x') = \max(\max\{W(x')_i : i \neq t\} - W(x')_t, -k) \quad (7)$$

$W(x')$ is the classification result of the sample not computed by the softmax function, and the added perturbation information is adjusted by setting the value of confidence k.

The difference between the normal sample and the adversarial sample is defined as in Equation (8):

$$r_n = \frac{1}{2}(\tanh(w_n) + 1) - X_n \quad (8)$$

The total results of the confusion matrix when the victim network is a DBN are shown in Figure 2. The comparison results in Figure 4 and Figure 5 show that the ASR of NITBA is 38.78% higher than the ASR of the

initial data, which indicates that the generated attack samples can masquerade as normal network behavior and bypass the victim network. It also verifies the significant effect of the attack method. Regarding the difference in ASR, both DeepFool and C&W, compared in this paper, can disguise the attack behavior data well. However, the quality of the attack samples generated by NITBA is still better than theirs, with ASRs 15.94% and 28.94% higher, respectively. In addition, NITBA takes much less time to generate attack samples than the other two methods.

When the victim network is LeNet-5, the total result of the confusion matrix is shown in Figure 3. The comparison of ASR and GTAS is also demonstrated in Figure 4 and Figure 5, which show the ASR of NITBA is 37.03% higher than the ASR of the initial data, and11.55% and 23.52 higher than DeepFool and C&W, respectively. Meanwhile, the GTAS of NITBA is also the shortest among the three. Therefore, the NITBA proposed in this paper can effectively attack the traffic defense algorithm based on deep learning, and the attack performance is better than DeepFool and C&W.

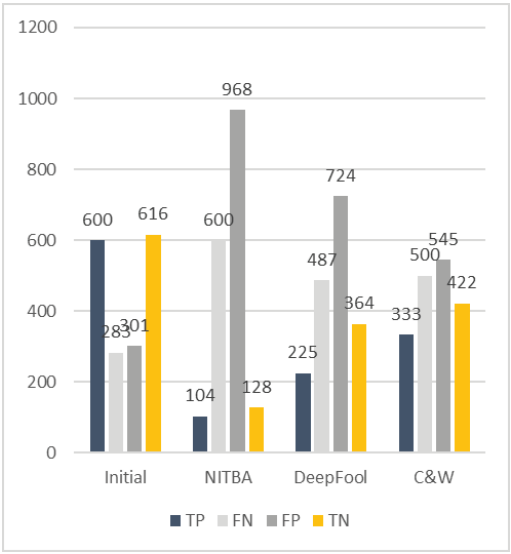


Figure 3: TP, FN, FP, TN (against LeNet-5)

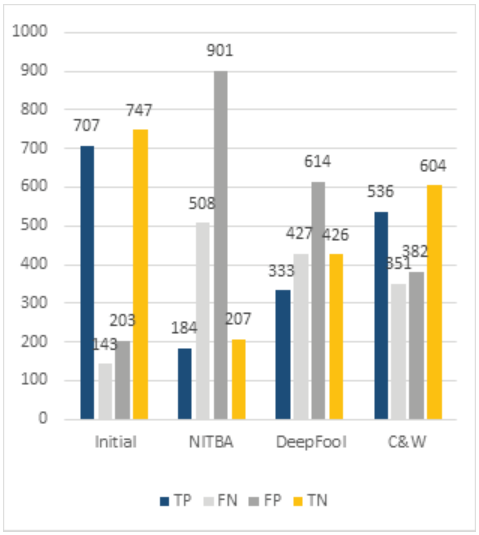


Figure 2: TP, FN, FP, TN (against DBN)

7 Conclusion

Deep neural network in deep learning has succeeded dramatically in many applications. Most existing backdoor attacks are against image processing and natural language processing, and to address this limitation, we propose a new backdoor attack called NITBA. It benefits from the random forest algorithm to classify the traffic with attack characteristics. It uses this as a basis to combine the non-attack characteristics of the generated samples with the attack characteristics of the attack behavior data to retain the attack capability of the generated samples to circumvent the classification of the target detection system and successfully bypass the other system. The exper-

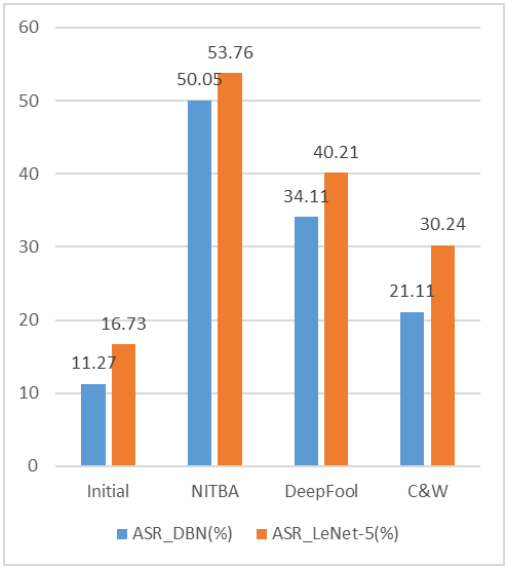


Figure 4: ASR

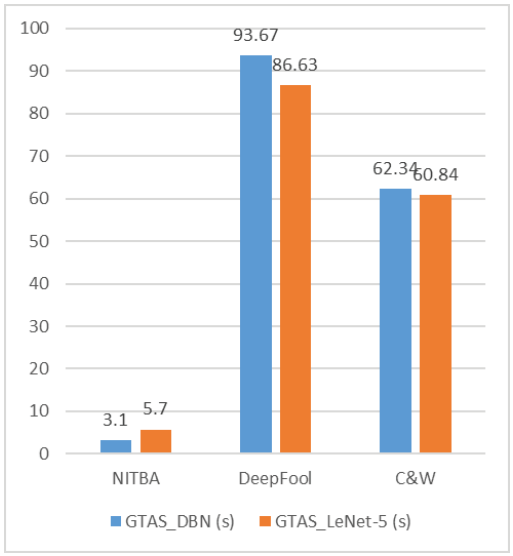


Figure 5: GTAS

iments show that the attack method generation proposed in this paper is more effective against the intrusion detection system based on a deep belief network, and the attack sample generation time is faster. Besides, Defense against traffic-based backdoor attacks is our future work.

Acknowledgments

This work was partly supported by the National key RD Program of China No. 2020YFC1522900; the Fundamental Research Funds for the Central Universities No. CZZ21001 and No. QSZ17007; and natural science foundation of Hubei Province under grants No. 2018ADC150 and the Innovation Fund for Postgraduates of South-Central Minzu University no. 3212023SYCXJJ162.

References

[1] A. Graves, A.-r. Mohamed, and G. Hinton, "Speech recognition with deep recurrent neural networks," in *2013 IEEE international conference on acoustics, speech and signal processing*. Ieee, 2013, pp. 6645–6649.

[2] T.-H. Chan, K. Jia, S. Gao, J. Lu, Z. Zeng, and Y. Ma, "Pcanet: A simple deep learning baseline for image classification?" *IEEE transactions on image processing*, vol. 24, no. 12, pp. 5017–5032, 2015.

[3] J.-X. Tong, H. Li, and S.-L. Yin, "Research on face recognition method based on deep neural network," *International Journal of Electronics and Information Engineering*, vol. 12, no. 4, pp. 182–188, 2020.

[4] T.-T. Gao, H. Li, and S.-L. Yin, "Adaptive convolutional neural network-based information fusion for facial expression recognition," *International Journal of Electronics and Information Engineering*, vol. 13, no. 1, pp. 17–23, 2021.

[5] T. Gu, K. Liu, B. Dolan-Gavitt, and S. Garg, "Badnets: Evaluating backdooring attacks on deep neural networks," *IEEE Access*, vol. 7, pp. 47 230–47 244, 2019.

[6] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," *arXiv preprint arXiv:1412.6572*, 2014.

[7] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, and R. Fergus, "Intriguing properties of neural networks," *arXiv preprint arXiv:1312.6199*, 2013.

[8] M. Kloft and P. Laskov, "Online anomaly detection under adversarial impact," in *Proceedings of the thirteenth international conference on artificial intelligence and statistics*. JMLR Workshop and Conference Proceedings, 2010, pp. 405–412.

[9] A. Shafahi, W. R. Huang, M. Najibi, O. Suciu, C. Studer, T. Dumitras, and T. Goldstein, "Poison frogs! targeted clean-label poisoning attacks on neural networks," *Advances in neural information processing systems*, vol. 31, 2018.

[10] W. Guo, B. Tondi, and M. Barni, "A master key backdoor for universal impersonation attack against dnn-based face verification," *Pattern Recognition Letters*, vol. 144, pp. 61–67, 2021.

[11] A. Turner, D. Tsipras, and A. Madry, "Label-consistent backdoor attacks," *arXiv preprint arXiv:1912.02771*, 2019.

[12] K. Kurita, P. Michel, and G. Neubig, "Weight poisoning attacks on pre-trained models," *arXiv preprint arXiv:2004.06660*, 2020.

[13] X. C. A. Salem and M. B. S. M. Y. Zhang, "Badnl: Backdoor attacks against nlp models," *arXiv preprint arXiv:2006.01043*, 2020.

[14] S.-M. Moosavi-Dezfooli, A. Fawzi, and P. Frossard, "Deepfool: a simple and accurate method to fool deep neural networks," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016, pp. 2574–2582.

[15] N. Carlini and D. Wagner, "Towards evaluating the robustness of neural networks," in *2017 ieee symposium on security and privacy (sp)*. Ieee, 2017, pp. 39–57.

[16] E. Bagdasaryan, A. Veit, Y. Hua, D. Estrin, and V. Shmatikov, "How to backdoor federated learning," in *International Conference on Artificial Intelligence and Statistics*. PMLR, 2020, pp. 2938–2948.

[17] E. Bagdasaryan and V. Shmatikov, "Blind backdoors in deep learning models," in *Usenix Security*, 2021.

[18] S. S. Jajoo and K. A. Kumar, "A review on deep-learning based network intrusion detection systems," *International Journal of Electronics and Information Engineering*, vol. 13, no. 4, pp. 170–179, 2021.

[19] B. Chen, W. Carvalho, N. Baracaldo, H. Ludwig, B. Edwards, T. Lee, I. Molloy, and B. Srivastava, "Detecting backdoor attacks on deep neural networks by activation clustering," *arXiv preprint arXiv:1811.03728*, 2018.

[20] Y. Gao, C. Xu, D. Wang, S. Chen, D. C. Ranasinghe, and S. Nepal, "Strip: A defence against trojan attacks on deep neural networks," in *Proceedings of the 35th Annual Computer Security Applications Conference*, 2019, pp. 113–125.

[21] Y. Li, T. Zhai, B. Wu, Y. Jiang, Z. Li, and S. Xia, "Rethinking the trigger of backdoor attack," *arXiv preprint arXiv:2004.04692*, 2020.

[22] B. Wang, Y. Yao, S. Shan, H. Li, B. Viswanath, H. Zheng, and B. Y. Zhao, "Neural cleanse: Identifying and mitigating backdoor attacks in neural networks," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 707–723.

[23] J. Lin, L. Xu, Y. Liu, and X. Zhang, "Composite backdoor attack for deep neural network by mixing existing benign features," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020, pp. 113–131.

[24] G. E. Hinton, S. Osindero, and Y.-W. Teh, "A fast learning algorithm for deep belief nets," *Neural computation*, vol. 18, no. 7, pp. 1527–1554, 2006.

[25] Y. LeCun *et al.*, "Lenet-5, convolutional neural networks," *URL: http://yann. lecun. com/exdb/lenet*, vol. 20, no. 5, p. 14, 2015.

[26] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, p. e4150, 2021.

[27] F. Mercaldo and A. Santone, "Deep learning for image-based mobile malware detection," *Journal of Computer Virology and Hacking Techniques*, vol. 16, no. 2, pp. 157–171, 2020.

[28] J. Chen, Z. Yu, and Z. Gu, "Semi-supervised deep learning in motor imagery-based brain-computer interfaces with stacked variational autoencoder," in *Journal of Physics: Conference Series*, vol. 1631(1). IOP Publishing, 2020, p. 012007.

[29] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, "A detailed analysis of the cicids2017 data set," in *Information Systems Security and Privacy: 4th International Conference, ICISSP 2018, Funchal-Madeira, Portugal, January 22-24, 2018, Revised Selected Papers 4*. Springer, 2019, pp. 172–188.

Biography

Jiahui Wang was born in 1999 and is now a postgraduate at the school of computer science,South-Central Minzu University,China. Her current research interests include cyber security and blockchain.

Jie Yang was born in 1996 and received his M.S. degree at the school of computer, South-Center Minzu University, China. Now he is a network security management engineer.

Binhao Ma was born in 1997 and is now a postgraduate at the school of computer science,South-Central Minzu University,China. His current research interests include cyber security and blockchain.

Dejun Wang was born in 1974 and received his Ph.D. in information security at Wuhan University in China. Currently, he is an associate professor at the school of computer science, South-Center Minzu University, China. He has authored/co-authored over 20 papers in international/national journals and conferences. His current research interests include security protocols and formal methods.

Bo Meng was born in 1974 in China. He received his M.S. in computer science and technology in 2000 and his Ph.D. degree in traffic information engineering and control from Wuhan University of Technology in Wuhan, China in 2003. From 2004 to 2006, he worked at Wuhan University as a postdoctoral researcher in information security. Currently, he is a full Professor at the school of computer science, South-Center Minzu University, China. He has authored/coauthored over 50 papers in International/National journals and conferences. In addition, he has also published a book, "secure remote voting protocol," in the science press in China. His current research interests include Cyberspace security.

A Lightweight and Flexible Privacy-preserving Electricity Theft Detection Scheme

Zining Zheng[1], Siliang Dong[2], and Yining Liu[2]
(Corresponding author: Yining Liu)
College of Computer and Information Science, Southwest University, Chongqing 400715, China[1]
School of Computer and Information Security, Guilin University of Electronic Technology, Guilin 541004, China[2]
Email: lyn7311@sina.com
(Received Oct. 30, 2022; Revised and Accepted June 2, 2023; First Online June 25, 2023)

Abstract

The theft of electricity is widespread in smart grids, which will cause significant losses to the electricity supplier. Therefore, electricity theft detection is necessary. Most electricity theft detection schemes are mainly based on machine learning methods. These schemes consider the detector to be trusted. However, in reality, detectors are often untrusted, so directly publishing user data to the machine learning detector will leak user privacy, making the detection system less robust. Some other methods of machine learning-based electricity theft detection in which the authors consider the detector to be untrusted, although the protection of user privacy is achieved; however, among these schemes that treat the detector as untrusted, some schemes are only suitable for a fixed model, which lacks flexibility, and some schemes, such as federated learning, have too much interaction. Thus the computational burden and communication burden is too heavy. Moreover, the above scheme, whether the detector is considered trusted or untrusted, is to detect individual users, so it needs to store and detect massive amounts of data, which makes the system lack lightweight. In this paper, we propose a scheme that combines data aggregation and convolutional neural networks (CNN) to detect the number of users stealing electricity in a group. In the detection process, group users submit aggregated values for detection, thereby effectively protecting the data privacy of a single user. The accuracy of the existing mainstream electricity stealing detection schemes that directly detects whether a single user is stealing electricity can reach about 92.67%, our scheme protects user privacy at the cost of losing about 2.68% of the accuracy and adapts to multiple detection models, thus ensuring flexibility, and since our detection system only needs to store and detect the aggregate value of group users, our scheme is more lightweight.

Keywords: Convolutional Neural Networks; Data Aggregation; Electricity Theft Detection; Privacy

1 Introduction

Electricity theft occurs from time to time in the smart grid [2, 7], illegal users achieve the purpose of reducing electricity bills through the theft. Electricity theft not only severely disrupts the normal order of residents' electricity use, causes huge economic losses to power supply companies [28], and seriously damages state-owned assets, but also the safety of the electricity theft process is not guaranteed and poses a threat to the lives of the thieves. At the same time, electric stealing methods such as unauthorized connection of lines can easily cause accidents such as electric shock and fire [18], posing a serious threat to the lives and property safety of the surrounding people. Therefore, it is important to conduct electricity theft detection [1]. With the popularization of smart meters [24], users can interact with the data center in real time and upload real-time electricity consumption data to the data center [10], which provides favorable conditions for electricity theft detection based on data analysis methods [6]. The data center releases the data to the detector for detection, which can identify users suspected of stealing electricity.

In recent years, academia has done a lot of related research on electricity theft detection. The existing electricity theft detection methods are mainly divided into three categories: state estimation [30], game theory [3], and machine learning [17]. Among them, machine learning is the most commonly used method. Through machine learning, users who are suspected of stealing electricity can be quickly locked, thereby greatly reducing the cost of manual investigation. However, the existing most detection schemes based on machine learning treat the detector as trusted, and do not perform any privacy treatment before submitting the user data to the detector, which is likely to expose user privacy. For example, in [34], the author uses a depth and width convolutional neural network to identify users who steal electricity [31]. The detector directly obtains the original data corresponding to the user, which exposes user privacy [27]. In [32], the author uses

a combined convolutional neural network to extract the electricity consumption features of a single user and other users in nearby areas through the convolution layer [8]. These features are then combined to learn the correlation of the electricity consumption patterns between a single user and other users in nearby areas, thereby improving the accuracy of detecting electricity theft users. However, this scheme still considers the detector to be trusted, the detector can directly obtain the plaintext of the user's electricity consumption data by decrypting the ciphertext. In reality, the detector is often untrusted, so there is a risk of leaking user privacy. The above schemes all improve the detection accuracy by modifying the machine learning model, and they do not take into account the protection of user data privacy. In some other methods of machine learning-based electricity stealing detection in which the authors consider the detector to be untrusted, although the protection of user privacy is achieved, it is only suitable for fixed model detection [20,22], thus lack of flexibility, and some other schemes have too much interaction, thus the computational burden and communication burden are too heavy [29]. For example, in [22], malicious behaviour is detected by calculating the euclidean distance between energy output measurements from an installation over a day, and this method is only applicable to clustering models. In [20], the scheme can realize the detection of ciphertext data through the combination of support vector machine (SVM) and homomorphic encryption. Since the detected data is in ciphertext state, user privacy is protected, but this method is only applicable to support vector machine. In [29], the authors use the federated learning method to detect electricity theft and protect user privacy, but the computational burden and communication burden are too heavy. All in all, in the past electricity theft detection schemes, some schemes regard the detector as trusted and do not protect user privacy, and some schemes regard the detector as untrusted, although user privacy is protected, but they lack flexibility and the communication burden are too heavy. Moreover, the above schemes are all for individual user detection, which requires storage and detection of massive data, resulting in an excessive burden of system storage and detection. Therefore, the above schemes lack lightweight. In order to guarantee the privacy and lightweight and flexibility of the system, the data should be privately processed first, and then published to the detector for detection [19]. The existing data privacy processing technologies mainly include n-source anonymous raw data collection protocols [5, 13, 33], data aggregation [12, 25] and other methods. In [5], the author assigns slots to users through the $shuffle$ method, and the slot assigned to a user is only known to the user. The users upload data through the assigned slots to ensure the rawness and unlinkability of the data. Although processing data through the n-source anonymity method ensures user privacy, but due to the storage burden, n-source anonymity is not suitable for use in scenarios with a large amount of data. Inspired by the COVID-19 dilution mixed sample detection technology [15], which is used by the National Health Commission to screen large-scale populations, and mixed multiple specimens for preliminary screening, thereby improving detection efficiency and reducing detection costs, we propose a privacy-preserving scheme to detect the number of users stealing electricity in a group.

In our scheme, an important attribute of electricity consumption behavior of users is considered: that is periodicity, which means the users usually consume energy cyclically (daily or weekly) [32, 34]. Therefore, the group of neighboring users generally meets the periodicity of electricity consumption. For example, if several users on a floor are regarded as a group, the overall electricity consumption feature of the group should also meet periodicity. If there are users stealing electricity in a group, it will destroy the periodic electricity consumption feature of the group. We use convolutional neural networks to analyze the overall long-term electricity consumption pattern of the group, identify some groups with abnormal electricity consumption feature, and predict the number of electricity theft users in the group based on the degree of abnormality. Combining data aggregation and machine learning, the data of a single user is covered by the aggregation value of group data to protect user privacy. The storage burden is greatly reduced, and the electricity theft detection is completed at the same time. In this paper, our proposed scheme has the following contribution points.

1) An electricity theft detection scheme that guarantees flexibility and privacy without the need for a trusted detector is proposed.

2) We proposed a group user electricity theft detector, selecting a reasonable number of people to form a group for detection, our detection system only needs to store and detect the aggregate value of group users, which reduces the storage burden and makes the detection system more lightweight.

3) We have conducted extensive experiments on massive realistic electricity consumption datasets. Experiments show that our scheme guarantees the lightweight, flexibility and privacy of the detection system at the cost of losing about 2.68% of the accuracy.

2 Preliminaries

A. Paillier Homomorphic Algorithm

Paillier homomorphic algorithm is a homomorphic algorithm widely used in the field of privacy protection, mainly divided into 5 parts, see [16] for details.

1) Generation of homomorphic key: Choose a security parameter κ and two large prime numbers p and q, where $|p| = |q| = k$. Compute the parameters $n = pq$, $\lambda = lcm(p-1, q-1)$ and select the element $g \in$

$z^*_{n^2}$. Set the public key to (n, g) and private key to λ. Define the function:

$$L(\varnothing) = (\varnothing - 1)/n$$

2) Encryption: Choose a random number $r_i \in z^*_{n^2}$, encrypt the plaintext m_i, get the ciphertext $c_i = E(m_i) = g^{m_i} r_i^n$.

3) Decryption: Decrypt ciphertext c_i into plaintext m_i:

$$m_i = D(c_i) = \frac{L\left(c_i^{\lambda} \bmod n^2\right)}{L\left(g^{\lambda} \bmod n^2\right)} \bmod n.$$

4) Aggregate multiple ciphertexts $c_i = E(m_i) = g^{m_i} r_i^n$, $1 \le i \le w$, as follows:

$$c = \prod_{i=1}^{w} c_i \bmod n^2 = \prod_{i=1}^{w} g^{m_1+m_2+\cdots+m_n} r_i^n \bmod n^2.$$

5) Decrypt the aggregated ciphertext:

$$m = \frac{L\left(c^{\lambda} \bmod n^2\right)}{L\left(g^{\lambda} \bmod n^2\right)} \bmod n, m = m_1 + m_2 + \cdots + m_n.$$

B. MinMaxScaler

MinMaxScaler is one of the methods of data normalization, which is a linear transformation of the original data. It normalizes the data to $[0, 1]$, so that the features of different dimensions are at the same numerical magnitude, reducing the impact of features with large variances on the prediction results, speeding up model convergence, and improving model accuracy. The equation is as follows:

$$\hat{x} = \frac{x - min}{max - min}.$$

Among them,x is the original value to be transformed currently,min is the minimum value in the current feature,max is the maximum value in the current feature, and $\hat{x}$ is the new value after transformation.

C. Principal Component Analysis

Principal Component Analysis(PCA) is a method of simplifying datasets [21]. It is often used for dimensionality reduction of high-dimensional datasets. It can be used to extract the main feature components of the data and reduce the dimensionality of the dataset while maintaining the feature that contributes the most to the variance of the dataset. In dimensionality reduction, the information measurement indicator used by PCA is the sample variance, the feature variance equation is as below:

$$v_{ar} = \frac{1}{n-1} \sum_{i=1}^{n} (x_i - \hat{x})^2.$$

Where v_{ar} represents the variance of a feature, n represents the number of samples, x_i represents the value of each sample in a feature, and $\hat{x}$ represents the mean of this list of samples.

D. Convolutional neural network

Convolutional neural network (CNN) is a feedforward neural network that includes convolution calculations and has a deep structure. It is good at processing images, especially large-scale image related machine learning problems [4]. It is one of the representative algorithms of deep learning. CNN includes convolutional layers, pooling layers, and full connection layers [4]. The internal structure of CNN is shown as Figure 1.

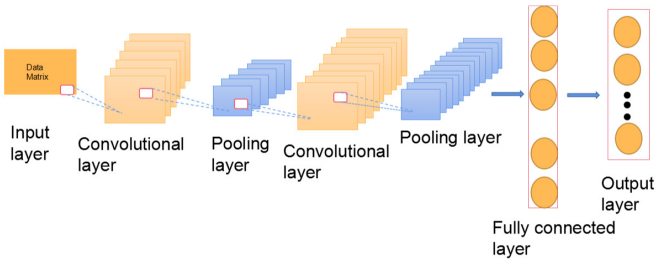


Figure 1: Classic CNN structure diagram

The core of CNN is feature learning, which obtains hierarchical feature information through a hierarchical network, so as to solve the important problem of manual design of features in the past. Each convolutional layer in a convolutional neural network consists of several convolutional units, and the parameters of each convolutional unit are optimized through backpropagation.

The purpose of the convolution operation is to extract different features of the input. The first layer of convolution may only extract some low-level features, such as edges, lines, and corners. More layers of the network can iteratively extract more complex features from low-level features. The pooling layer is a form of downsampling. The pooling layer will continuously reduce the size of the data space, so the number of parameters and the amount of calculation will also decrease, which controls the overfitting of the model to a certain extent.

Each node of the full connection layer is connected to all the nodes of the previous layer, used to integrate the features extracted from the previous layer, and integrate the category-discriminatory information in the convolutional layer or the pooling layer, and finally the probability of the categories are output by the softmax function.

3 System Model and Privacy Threats

3.1 System Model

As shown in Figure 2, the system model includes users U_i, $i \in [1, n]$, fog nodes (FN), cloud server (CS), and the electricity theft detector.

1) The electricity theft detector receives data from the cloud server for electricity theft detection.

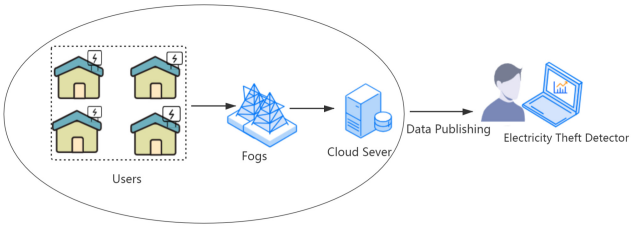


Figure 2: System model

2) Each user's home is equipped with a smart meter, and the smart meter uploads the user's real-time power consumption data to FN.

3) FN is a device deployed at the edge of the user, which replaces the CS to perform part of the calculation to reduce the computing burden of the CS. It acts as an aggregator here, which aggregates the electricity consumption data of regional users and transmits it to the CS according to the rules of [11, 14].

4) After receiving the data from FN, the CS outsources the data to the electricity theft detector for electricity theft detection.

3.2 Privacy Threats

There are a series of security problems in the smart grid, such as data injection attack, the denial of service attack, and some other physical threats [23]. The traditional security goal is to ensure that data can only be shared between authorized parties, and unauthorized parties can not get anything, so encryption technology is mainly used to achieve this. The authorized party can decrypt the encrypted ciphertext to get the plaintext, but the unauthorized party can not get anything. However, such security measures are not feasible for our current scheme. As an external party of the power system, the detector is untrusted and obviously not an authorized party. Therefore, it can not get the user's raw data, but if the encrypted ciphertext is given to the detector, due to the complete independence between the ciphertext and the plaintext, the ciphertext does not contain any features of the plaintext, and the detector certainly can not detect anything.

Therefore, different from traditional security goals, our privacy goals require us to process the data like this: on the one hand, we must eliminate some features to make the published data private, and on the other hand, we must retain some features so that it can still be analyzed and used. In our scheme, the detector is untrusted. In order to protect user privacy, we eliminate the electricity consumption features of individual users by data aggregation, and retain the electricity consumption features of group users. What we release to the detector is the group's electricity consumption data, while protecting the privacy of individual users, the detector can still identify the number of electricity theft users in the group through analysis of the group's electricity consumption features. We assume that there is a secure communication channel between authorized entities, so we only consider privacy issues in our scheme, so there are the following privacy threats in our scheme:

1) Electricity theft detectors are untrusted and will sell the obtained data to other institutions or individuals for profit.

2) CS and FN are honest but curious. They will not tamper with user data, but will try to infer valuable information from the data.

3) Users are also honest but curious. They will follow the protocol honestly, but they will try to spy on the privacy of other users' electricity data.

4 Our Proposed Scheme

This section mainly describes the details of our scheme, including the electricity consumption privacy preservation part and the data detection part. In the electricity consumption privacy preservation part, we use the data aggregation method to obtain the aggregate value of the electricity consumption data of the user group, thereby protecting the data privacy of a single user. In the data detection part, an important attribute of electricity consumption behavior of users is considered: that is periodicity, which means the users usually consume energy cyclically (daily or weekly). We convert the user's electricity consumption data into a feature matrix in terms of cycles. The convolution kernel sliding of the convolutional neural network can well extract the potential law within the cycle of the electricity consumption data and the potential law between the cycle and the cycle. Therefore, the convolutional neural network can be well adapted to the periodic electricity consumption data detection. Therefore, in the data detection part, the model we use is convolutional neural network. We use convolutional neural networks to analyze the electricity consumption behavior patterns of group users over a long period of time, so as to identify groups that may have electricity theft users.

Part 1: Electricity Privacy Preservation

1) The cloud server starts to perform the Paillier encryption algorithm and selects the security parameter γ and choose two large prime numbers p and q, where $|p| = |q| = k$. Compute two parameters $n = pq$, $\lambda = lcm(p-1, q-1)$, and select the element $g \in z_{n^2}^*$, then set the public key to (n, g) and private key to (λ).

2) The user $U_i, i \in (1, 2, \cdots, w)$ chooses a random number and encrypt its electricity consumption data m_i, as follows?

$$c_i = E(m_i) = g^{m_i} r_i^n.$$

Then the user sends the encrypted electricity consumption data c_i to the FN.

3) When FN receives the user's encrypted electricity consumption data $c_i, i \in (1, 2, \cdots, w)$, FN aggregates them into c, as follows:

$$c = \prod_{i=1}^{w} c_i \bmod n^2 = g^{m_1+m_2+\cdots+m_w} (\prod_{i=1}^{w} r_i^n) \bmod n^2.$$

Then FN sends the ciphertext c to the CS.

4) When CS receives the ciphertext c, the CS decrypts it, as shown below:

$$m = \frac{L\left(c^{\lambda} \bmod n^2\right)}{L\left(g^{\lambda} \bmod n^2\right)} \bmod n, m = m_1 + m_2 + \cdots + m_w.$$

After the cloud server obtains the total electricity consumption data of the user group, it publishes the group electricity consumption data to the electricity theft detector for data detection.

Part 2: Data Dectection with Our Proposed Group User

A. Data Preprocessing

An electricity consumption dataset contains m samples, each sample contains the electricity consumption data of a user for n days, the last column of the dataset is the label corresponding to the user data, 0 represents normal users, 1 represents suspected electricity theft user. We randomly shuffle the samples of the electricity consumption dataset, reconstitute a group with s adjacent users, combine the n-day electricity consumption data of s users into n-day electricity consumption data of a group. If the label of each user in the group is 0, then the group is labeled as 0, which means that all users in the group are normal users. If there is a user in the group whose label is 1, then the group will be labeled 1, which means that there is a user suspected of stealing electricity in the group. If there are two users in the group whose label is 1, tag the group as 2, which means that there are two users suspected of stealing electricity in the group. By analogy, the reconstituted groups are labeled, so that we can obtain w labeled groups containing s users, where $w = w/s$, and each group sample contains the electricity consumption data of the group for n days.

In order to reduce the impact of the large variance of the group electricity data on the prediction results, we use the MinMaxScaler method to compress the features to the range of $[0, 1]$. Since the electricity consumption dataset contains the electricity consumption data of users for many days, we use the PCA method to reduce the dimensionality of the dataset, and then convert the group electricity consumption data into a matrix of dimension (p, q, d). p represents the number of rows of the matrix, q represents the number of columns of the matrix, and d represents the number of matrices. The matrix shape of a group is $(p, q, 1)$, as shown below:

$$\begin{pmatrix} [C_{1,1}] & \cdots & [C_{1,q}] \\ \vdots & \ddots & \vdots \\ [C_{p,1}] & \cdots & [C_{p,q}] \end{pmatrix}$$

B. Our CNN Model

We use 3 convolutional layers, 3 pooling layers and a full connection layer to build our CNN model, as shown in Figure 3, including 3 stages:

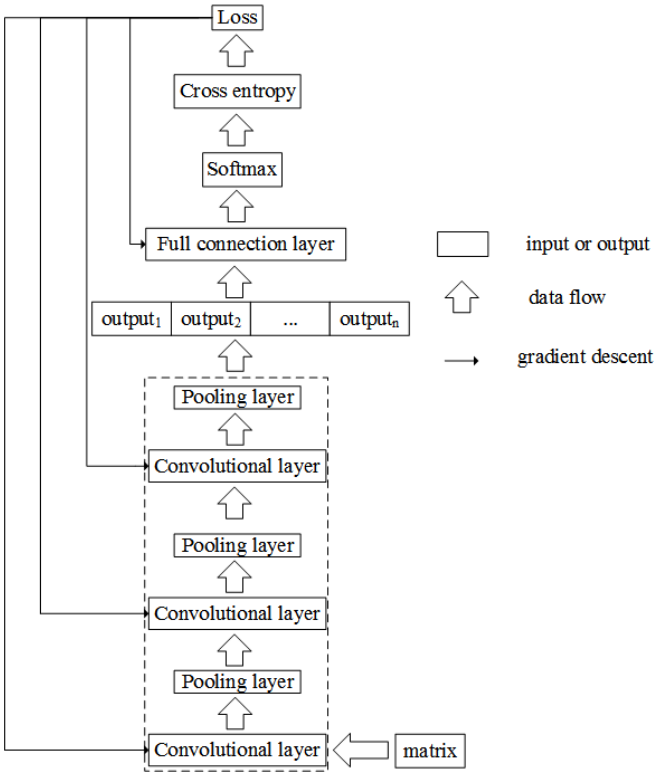


Figure 3: CNN model training flowchart

1) The input data should be $(j, c, 1)$ since the group data is input as a whole.

2) We use the convolutional layers to extract features, and the pooling layers filter out the main features. For example, the current feature matrix shape is (j, c, r). After passing through the convolutional layer containing convolution kernels, the matrix shape becomes (j, c, a) and after the pooling layer, the matrix shape becomes $(j/2, c/2, a)$.

3) After all convolution and pooling operations, we convert the features extracted by the convolutional layers and the pooling layers into a one-dimensional vector, and then use the full connection layer to synthesize the features. Then go through the softmax function, and the shape of the output vector is (β),

where $\beta = s + 1$. They are the probability that 0 user steals electricity in this group and the probability that 1 user steals electricity in this group, and the probability that s users steal electricity. Comparing the probabilities, output the maximum probability, then the number of users that the group may have for stealing electricity is the number corresponding to this maximum probability.

5 System Analysis

In this section, we analyze our detection system in two parts. The part 1 explains the privacy of the data, and in the part 2, we conduct experiments to prove that our data after privacy processing can still be used for electricity theft detection.

Part 1: Privacy Analysis

In this part, we analyze data privacy in the process of data collection and data publishing. Data collection refers to the process during which a user transmits data to FN, and then the FN transmits the data to CS. Data publishing refers to the process during which the CS transmits data to the detector.

1) The user $U_i, i \in (1, 2, \cdots, w)$ encrypt its electricity consumption data m_i into c_i, then user U_i sends the encrypted electricity consumption data c_i to the FN. When FN receives the ciphertext c_i, FN can not decrypt the ciphertext c_i to obtain the plaintext, so data privacy is protected in this process.

2) FN aggregates $c_i, i \in (1, 2, \cdots, w)$ into c, then FN sends the ciphertext c to the CS. When CS receives the ciphertext c_i, the CS decrypts c into m, where $m = m_1 + m_2 + \cdots + m_w$. m represents the sum of group electricity consumption data, so the CS can not get the data of a single user. Therefore, data privacy is protected in this process.

3) The CS publishes the group electricity consumption data m to the electricity theft detector for data detection. What the detector obtains are the aggregated values, the detector also can not get the data of a single user. So data privacy is protected in this process.

In summary, during the process of data collection and data publishing, no organization other than the user can obtain the user's raw data. Therefore, it can be proved that the data privacy is protected during the process of data collection and data publishing.

Part 2: Experients and Analysis

In the part, we prove that our data after privacy processing can still be used for electricity theft detection by conducting experiments on a 64-bit computer with Intel(R) Core(TM) i5-6500 CPU, 3.2GHz, 8GB RAM, using Python, Tensorflow and Keras framework.

A. Experiment Data

We use the labeled database from State Grid Corporation of China (SGCC) [32, 34] to conduct experiments. The SGCC dataset contains the energy usage data of 42372 customers within 1035 days, and the last column of the dataset is the label corresponding to the user, which is a single value (0 or 1), 0 represents the normal user, 1 represents the suspected electricity theft user.

The selection of the number of people in a group is important, since our scheme is to identify electricity theft by detecting whether the periodicity of the electricity consumption of the group are abnormal. The detection accuracy will decrease as the number of people in the group increases, since if there are too many people in a group, slight electricity theft will not have a significant impact on the periodicity of the electricity consumption of the group, and it will not be easy to detect electricity theft, thereby affecting the detection accuracy. If the number of people in a group is too small, untrusted detectors can still roughly infer the range of individual electricity consumption data from the group data, and data privacy can not be guaranteed.

Therefore, we must choose a reasonable number of people to form a group to balance data privacy and detection accuracy. In order to balance data privacy and detection accuracy, we randomly shuffle the samples of the SGCC dataset, reconstitute a group with 4 adjacent users, combine the 1035-day electricity consumption data of 4 users into 1035-day electricity consumption data of a group. If the label of each user in the group is 0, then the group is labeled as 0, which means that all users in the group are normal users. If there is a user in the group whose label is 1, then the group will be labeled as 1, which means that there is a user suspected of stealing electricity in the group. If there are two users in the group whose label is 1, tag the group as 2, which means that there are two users suspected of stealing electricity in the group. If there are three users in the group whose label is 1, tag the group as 3, which means that there are three users suspected of stealing electricity in the group. If there are four users in the group whose label is 1, then the group will be labeled as 4, which means that there are four users suspected of stealing electricity in the group.

In this way, we can obtain 10593 labeled groups containing 4 users, and each group contains 1035 days of electricity consumption data for the group. We randomly divide 80% as the training set and 20% as the test set. We use MinMaxScaler method to compress the group's electricity consumption data in the range of $[0, 1]$, and then use PCA to reduce the dimensionality of the dataset.

As shown in Figure 4, we can see that when the feature dimension is 245, the cumulative explainable variance ratio can still reach 99%. In other words, when the group

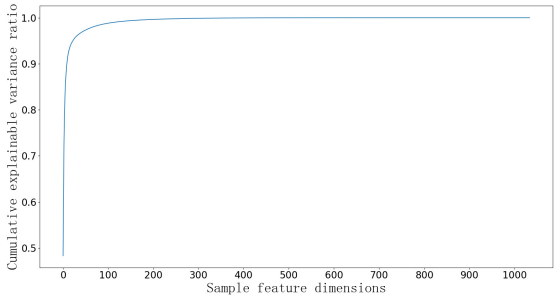


Figure 4: Cumulative explainable variance ratio

electricity consumption data is reduced to 245 dimensions, 99% of the feature information can still be retained. Then we convert the reduced dimensionality data into a matrix form of shape (35,7,1) by weekly cycle:

$$\begin{pmatrix} [C_{1,1}] & \cdots & [C_{1,7}] \\ \vdots & \ddots & \vdots \\ [C_{35,1}] & \cdots & [C_{35,7}] \end{pmatrix}$$

B. Model Training Phase

Our convolutional neural network contains 3 convolutional layers, 3 pooling layers, and 1 full connection layer. Our first convolutional layer contains 64 convolution kernels with a size of (5,5), and the sliding step size is (1,1), using the method of padding when doing convolution operation in the input matrix. The output of the first convolutional layer is a matrix whose shape is (35,7,64), and then the matrix is passed to the first pooling layer. We adopt the maximum pooling method, the sliding window size of the pooling layer is set to the size of (2,2), and the sliding step size is set to (2,2).

The output of the first pooling layer is a matrix whose shape is (18,4,64), and then the matrix is passed to the second convolution layer which contains 128 convolution kernels with a size of (5,5), and the sliding step size is (1,1), the output of the second convolution layer is a matrix whose shape is (18,4,128). And then the matrix is passed to the second pooling layer, the sliding window size of the pooling layer is set to the size of (2,2), the sliding step size is set to (2,2), the output of the second pooling layer is a matrix whose shape is (9,2,128). And then the matrix is passed to the third convolution layer which has 256 convolution kernels with a size of (5,5), the sliding step size is (1,1), the output of the third convolution layer is a matrix whose shape is (9,2,256). And then the matrix is passed to the third pooling layer, the sliding window size of the pooling layer is set to the size of (2,2), the sliding step size is set to (2,2), the output of the third pooling layer is a matrix whose shape is (5,1,256). Then expand the matrix into a (1,1280) vector. After that, it is passed to the full connection layer to synthesize the previous features, and the categories probabilities are output through the softmax function.

The predicted categories are compared with the real categories, and the parameters are continuously updated through gradient descent to optimize the model, this is the model training process.

C. Model Evaluation

We use accuracy as our model evaluation indicator, the equation is as follows:

$$accuracy(\hat{y}, y) = \frac{1}{n}\sum_{i=1}^{n}\delta(y_i, \hat{y}_i)$$

where $\delta(y_i, \hat{y}_i) = \begin{cases} 1, & y_i = \hat{y}_i; \\ 0, & else. \end{cases}$

The $\hat{y}$ represents the predicted value and the y represents the true value. $\hat{y}_i$ is the predicted value of the i-th sample and y_i is the corresponding true value, n represents the number of samples. We train the model for 100 epochs to update the model parameters. After training the model, we evaluate the model on the test set, the model accuracy score is 89.99%.

Table 1: Model accuracy comparison

Model	Arguments	Accuracy score
Combined CNN	100 epochs	0.9267
Logistic Regression	Penalty: L2	0.9140
Random Forest	Max depth: 7	0.9162
SVM	Kernel: nonlinear function	0.8975
Our scheme	100 epochs	0.8999

D. Model Comparision

We compare the designed group user electricity theft detector with the traditional individual user electricity theft detector, such as trusted Combined CNN detector [32], trusted Logistic Regression (LR) detector [9] and trusted Random Forest (RF) detector [26] and untrusted SVM detector [20]. Experiments show that our scheme with untrusted detectors has a loss in accuracy compared with schemes with trusted detectors, but the accuracy is higher than other schemes with untrusted detectors, as shown in Table 1.

E. Comparision with Existing Schemes

This section mainly describes the comparison between our scheme and the existing electricity theft detection scheme. In the scheme of Yao *et al.* [32], the detector is regarded as trusted, this scheme will leak user privacy, the detector can obtain the user's plaintext data, so as to realize the electricity distribution decision, and the model can continue to be optimized, so that the model has flexibility, to detect individual users, the detection system has a heavy burden and lacks lightweight. In the scheme of Zheng *et al.* [34], which is similar to Yao *et al.* [32], the detector

Table 2: Properties comparison

Features	Proposed scheme	Yao *et al.* [15]	Rechardson *et al.* [17]	Rahulamathavan *et al.* [18]	Zheng *et al.* [13]
Relying on trusted detectors	No	Yes	No	No	Yes
User privacy	Yes	No	Yes	Yes	No
Dispatching of smart grid	Yes	Yes	No	No	Yes
Model flexibility	Yes	Yes	No	No	Yes
Detection system lightweight	Yes	No	No	No	No

is trusted, user privacy is not protected, the sum of electricity consumption data can be obtained to realize electricity distribution decision and the model has room for further optimization, has flexibility, and lacks lightweight. Rechardson's [22] scheme considers the detector to be untrusted, but can not realize the dispatch in the smart grid since the control center can't obtain the total electricity consumption data by sending euclidean distance to the operator, and for clustering models only, thus lack of model flexibility, to detect individual users, the detection system has a heavy burden and lacks lightweight too. Rahulamathavan's [20] scheme considers the detector to be untrusted, but also can not realize the dispatch in the smart grid since user data is encrypted throughout, and for support vector machine models only, thus lack of flexibility, to detect individual users, so there is also the problem of lacking lightweight. Our scheme treats the detector as untrusted and adapts to multiple detection models, the detector detects the aggregated data of a group, so as to detect the number of users stealing electricity in the group. We protect the privacy of a single user through the data aggregation. After the detector obtains the electricity consumption data of the groups, it aggregates the electricity consumption data of multiple groups to obtain the sum of the regional electricity consumption data, so as to make a decision on the regional electricity distribution. From Table 2, we can see that our scheme dose not rely on trusted detectors, and can guarantee user privacy and the lightweight of the detection system, adapt to multiple detection models, make decisions about electricity distribution.

6 Conclusions

In this paper, we propose a lightweight and flexible privacy-preserving detection scheme for electricity theft. In our scheme, we aggregate user data to detect the number of users stealing electricity in a group, and protect the data privacy of a single user. Moreover, our scheme reduces the data storage and detection burden of the detection system, and is also applicable to multiple detection models, thus ensuring the lightweight and flexibility of the detection system. However, our detection accuracy still has room for improvement. In our future work, we will consider optimizing our model to improve detection accuracy.

Acknowledgments

This study was supported by *****. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] M. S. Ballal, H. Suryawanshi, M. K. Mishra, and G. Jaiswal, "Online electricity theft detection and prevention scheme for smart cities," *IET Smart Cities*, vol. 2, no. 3, pp. 155–164, 2020.

[2] P. P. Biswas, H. Cai, B. Zhou, B. Chen, D. Mashima, and V. W. Zheng, "Electricity theft pinpointing through correlation analysis of master and individual meter readings," *IEEE Transactions on Smart Grid*, vol. 11, no. 4, pp. 3031–3042, 2019.

[3] A. A. Cárdenas, S. Amin, G. Schwartz, R. Dong, and S. Sastry, "A game theory model for electricity theft detection and privacy-aware control in ami systems," in *2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE, 2012, pp. 1830–1837.

[4] G. Chen, Y. Chen, Z. Yuan, X. Lu, X. Zhu, and W. Li, "Breast cancer image classification based on cnn and bit-plane slicing," in *2019 International Conference on Medical Imaging Physics and Engineering (ICMIPE)*. IEEE, 2019, pp. 1–4.

[5] J. Chen, G. Liu, and Y. Liu, "Lightweight privacy-preserving raw data publishing scheme," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 4, pp. 2170–2174, 2020.

[6] M. Chen, R. Shi, and B. He, "Noise threshold estimation in spectrum monitoring data analysis application," in *2018 IEEE 3rd International Conference on Big Data Analysis (ICBDA)*. IEEE, 2018, pp. 242–247.

[7] I. Colak, R. Bayindir, and S. Sagiroglu, "The effects of the smart grid system on the national grids," in *2020 8th International Conference on Smart Grid (icSmartGrid)*. IEEE, 2020, pp. 122–126.

[8] F. Haider, S. Pollak, P. Albert, and S. Luz, "Extracting audio-visual features for emotion recognition through active feature selection," in *2019 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*. IEEE, 2019, pp. 1–5.

[9] D. W. Hosmer, T. A. Hosmer, S. le Cessie, and S. Lemeshow, "A comparison of goodness-of-fit tests for the logistic regression model." *Statistics in medicine*, vol. 16 9, pp. 965–80, 1997.

[10] L. Jiadi, H. Yang, L. Huan, Z. Xinli, and L. Wen-Jing, "Research on data center operation and maintenance management based on big data," in *2020 International Conference on Computer Engineering and Application (ICCEA)*. IEEE, 2020, pp. 124–127.

[11] Y. Lin and H. Shen, "Cloud fog: Towards high quality of experience in cloud gaming," *2015 44th International Conference on Parallel Processing*, pp. 500–509, 2015.

[12] Y. Liu, W. Guo, C.-I. Fan, L. Chang, and C. Cheng, "A practical privacy-preserving data aggregation (3pda) scheme for smart grid," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1767–1774, 2018.

[13] Y.-N. Liu, Y.-P. Wang, X.-F. Wang, Z. Xia, and J.-F. Xu, "Privacy-preserving raw data collection without a trusted authority for iot," *Computer Networks*, vol. 148, pp. 340–348, 2019.

[14] L. Lyu, K. Nandakumar, B. I. P. Rubinstein, J. Jin, J. Bedő, and M. S. Palaniswami, "Ppfa: Privacy preserving fog-enabled aggregation in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 14, pp. 3733–3744, 2018.

[15] M. Mishra, V. Parashar, and R. Shimpi, "Development and evaluation of an ai system for early detection of covid-19 pneumonia using x-ray (student consortium)," in *2020 IEEE Sixth International Conference on Multimedia Big Data (BigMM)*. IEEE, 2020, pp. 292–296.

[16] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology—EUROCRYPT'99: International Conference on the Theory and Application of Cryptographic Techniques Prague, Czech Republic, May 2–6, 1999 Proceedings 18*. Springer, 1999, pp. 223–238.

[17] J. Pereira and F. Saraiva, "A comparative analysis of unbalanced data handling techniques for machine learning algorithms to electricity theft detection," in *2020 IEEE Congress on evolutionary computation (CEC)*. IEEE, 2020, pp. 1–8.

[18] J. Presnal, H. Houston, and G. Maberry, "The electrical safety program and the value in parterning with health & safety professionals," in *2020 IEEE IAS Electrical Safety Workshop (ESW)*. IEEE, 2020, pp. 1–7.

[19] R. Punmiya and S. Choe, "Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2326–2329, 2019.

[20] Y. Rahulamathavan, R. C.-W. Phan, S. Veluru, K. Cumanan, and M. Rajarajan, "Privacy-preserving multi-class support vector machine for outsourcing the data classification in cloud," *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 5, pp. 467–479, 2013.

[21] A. Rehman, A. Khan, M. A. Ali, M. U. Khan, S. U. Khan, and L. Ali, "Performance analysis of pca, sparse pca, kernel pca and incremental pca algorithms for heart failure prediction," in *2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*. IEEE, 2020, pp. 1–5.

[22] C. Richardson, N. Race, and P. Smith, "A privacy preserving approach to energy theft detection in smart grids," in *2016 IEEE International Smart Cities Conference (ISC2)*. IEEE, 2016, pp. 1–4.

[23] A. Sanjab, W. Saad, I. Güvenç, A. I. Sarwat, and S. K. Biswas, "Smart grid security: Threats, challenges, and solutions," *ArXiv*, vol. abs/1606.06992, 2016.

[24] T. Sirojan, S. Lu, B. T. Phung, and E. Ambikairajah, "Embedded edge computing for real-time smart meter data analytics," in *2019 International Conference on Smart Energy Systems and Technologies (SEST)*. IEEE, 2019, pp. 1–5.

[25] J. Song, Y. Liu, J. Shao, and C. Tang, "A dynamic membership data aggregation (dmda) protocol for smart grid," *IEEE Systems Journal*, vol. 14, no. 1, pp. 900–908, 2019.

[26] V. Svetnik, A. Liaw, C. Tong, J. C. Culberson, R. P. Sheridan, and B. P. Feuston, "Random forest: A classification and regression tool for compound classification and qsar modeling," *Journal of chemical information and computer sciences*, vol. 43 6, pp. 1947–58, 2003.

[27] N. Takbiri, A. Houmansadr, D. L. Goeckel, and H. Pishro-Nik, "Privacy of dependent users against statistical matching," *IEEE Transactions on Information Theory*, vol. 66, no. 9, pp. 5842–5865, 2020.

[28] S. Viktor, D. Oleksiy, B. Petro, K. Yevhen, L. Vitalij, and T. Drubetskaya, "Asymmetric power supply circuit design for electric rolling stock on the electrified dc rail," in *2020 IEEE 7th International Conference on Energy Smart Systems (ESS)*. IEEE, 2020, pp. 326–329.

[29] M. Wen, R. Xie, K. Lu, L. Wang, and K. Zhang, "Feddetect: a novel privacy-preserving federated learning framework for energy theft detection in smart grid," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6069–6080, 2021.

[30] M. Wen, D. Yao, B. Li, and R. Lu, "State estimation based energy theft detection scheme with privacy preservation in smart grid," in *2018 IEEE International Conference on Communications (ICC)*. IEEE, 2018, pp. 1–6.

[31] R. Xin, J. Zhang, and Y. Shao, "Complex network classification with convolutional neural network," *Tsinghua Science and technology*, vol. 25, no. 4, pp. 447–457, 2020.

[32] D. Yao, M. Wen, X. Liang, Z. Fu, K. Zhang, and B. Yang, "Energy theft detection with energy privacy preservation in the smart grid," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7659–7669, 2019.

[33] Y. Zhang, Q. Chen, and S. Zhong, "Privacy-preserving data aggregation in mobile phone sens-

ing," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 980–992, 2016.

[34] Z. Zheng, Y. Yang, X. Niu, H.-N. Dai, and Y. Zhou, "Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1606–1615, 2017.

Biography

Zining Zheng is an undergraduate student, her current research interest is information security protocol.

Siliang Dong is researching the artificial intelligence and privacy.

Yining Liu. The research interests of Yining Liu include the seurity and privacy of VANET, data aggregation, machine learning.

Geospacial Analysis on DNS Servers for Furher Classification of Indicator of Compromise

Ruo Ando[1] and Hiroshi Itoh[2]
(Corresponding author: Ruo Ando)
National Institute of Informatics[1]
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo, Japan
National Institute of Information and Communications Technology[2]
4-2-1 Nukui-Kitamachi, Koganei, Tokyo, Japan
Email: ruo@nii.ac.jp
(Received Oct. 3, 2022; Revised and Accepted June 1, 2023; First Online June 25, 2023)

Abstract

Recently, TI (Threat Intelligence) has acquired a significant presence in cyber security. A common form of TI is IoC (an indicator of compromise). This paper presents a novel application of geospatial analysis to refine IoC further. First, we cope with open-source IoC of Russian malicious cyber activity. In the first phase of analysis, we detected 30,285,322 DNS servers on the Internet and measured the geospatial distance between the DNS server and each IP address of IoC. By doing this, we can expose the nearest DNS servers to IP addresses in IoC. Second, based on the first phase result, we compared the distance of the DNS server and gateway ISP detected by traceroute. Among 294 IP addresses of IoC, We have detected 104 DNS servers nearer than the gateway ISP, which is helpful for the classification of IoC. Finally, we have characterized IP addresses in IoC by three distance ranges (0-400, 400-800, and 800-1200km). We have found that the distance range is informative for characterizing IP addresses of IoC. Furthermore, experimental results demonstrate apparent features of communication line usage type (such as Fixed Line and Web Hosting) by three distance ranges. We believe these three kinds of insights will shed new light on further refinement of the indicator of compromise.

Keywords: DNS; Gateway ISP; Geospatial Analysis; Indicator of Compromise

1 Introduction

1.1 TI and IoC

Cyber threat intelligence (TI) is information or insights on the current attacker's behavior. Indicator of compromise (IoC) is the one form of threat intelligence with a machine-readable data feed, including IP addresses, malicious domains, and file hashes [22]. Also, IoCs serve as evidence of forensic about potential intrusions on our network.

Threat intelligence is divided into three categories: open, shared, and paid. IoCs include several fields such as:

1) Burst egress/ingress network traffic;
2) Unusual behavior as privileged user account;
3) Geographical outliers;
4) DNS malformed requests.

These indicatored are adopted for the early detection of maliciou activity in addintion to the prevension of known threats. This paper proposes a new IoC indicator generated by geospatial analysis of DNS servers. We have detected the nearest DNS server for each IP address of IoC towards the more feature-rich cyber threat intelligence.

1.2 DNS Security

The Domain Name System (DNS) handles the correspondence between domain names and IP addresses. DNS provides the resolution of Domain name on the Internet. DNS is also responsible in network security for the distribution of reputaion. For example, DNS-based Block Lists operates as spam filter and blocker of malicious web pages.

Attackers recognize DNS servers as tempting target. Unfortunately, the DNS protocol was not implemented with security as a top priority and therefore it has contained several limitation about security design. DNS are vulnerable to a wide range of spectrum of attacks. Attacks includes DOS (Denial of Service), spoofing, amplification and theft of private or confidintial information. Also, attachker can exploit a number of ways to compromise DNS severs still now. In the crisis of the DNS amp

attack around 2015, administrators forced to check the configuration of their DNS servers.

For these reasons, DNS server security is important for both administrators and clients. Administrators should block malicious DNS queries in order not to assist in cyber attacks. Clients should not choose or connect malicious DNS servers so that they are not involved in malicious cyber activities.

2 Russian Advanced Persistent Threat

Russian malicious cyber activity dates back to moonlight maze in 1999 [6]. In the 2010s, Russian cyber activities are gaining momentum. The Russian government supports malicious activities to control social and political activity, steal IP (intellectual property), and operate against regional and nationwide adversaries over a large geographic area. Besides, recently, the activities of cyber espionage have been increasing. According to CISA, Russian malicious cyber activities include SolarWinds software supply chain (2020), targeting developers of COVID-19 vaccines, and leaking of documents of the Democratic National Committee (2016). In this paper, we introduce an IoC, which is released as open-source concerning Russian malicious cyber activity. Grizzly Steppe is the nickname of the malicious activity by Russian intelligence services [19]. The IoC is based on a report published by DHS (Department of Homeland Security) and FBI (Federal Bureau of Investigation) in 2016. JAR refers to Grizzly Steppe as part of RIS (Russian civilian and military Intelligence Services) activities. In this paper, we cope with 294 IP addresses in IoC from Joint Analysis Report [5], which is released on December 29, 2016.

3 Geospatial Analysis

Geospatial data is information about a geographic aspect or positioning. Geospatial data has coordinates or an address associated with it, something that indicates its position in space. Geospatial data is used for the providing the detailed descripton of targets, events and other fueatres by a poision on or near the surface of the earch Also Geospatial data usually combines location information and attribute information with temporal information.

Geospatial analysis is based on the implementation of geospatial data into pre-existing security systems and can be a seamless way to strengthen cybersecurity. By integrating live location information into sophisticated cybersecurity systems, we can act quickly in response to current conditions, threats, and crises. First of all, we use geospatial data to prioritize cyber threats by quickly creating a solution that integrates multiple intelligence information analyses, sharing, and solutions. Cyber attacks have become more sophisticated by using a large number of hosts which is spreadly widely over the world.

Having a geographical view of networks enables us security administrators to get more detailed perspective on the pattern of attacks. For example, notification of certain organizations over a given geographical area, security administrators can better respond with geospacial analysis. Then we can minigate the attacks on the next victims based on attack patters found.

In this paper, we apply geospatial analysis based on the location of the DNS server for more profound insights of the IoC of Russian malicious cyber activity. Geospatial analysis is practical by appending information of DNS to each IP address of IoC.

Figure 1 shows the flow chart of our system. For geospatial analysis, we have two data sources:

1) crawling the Internet for obtaining the list of DNS servers.

2) open source IoC including the list of IP addresses.

For handling these two lists, we have two machines. One is for fetching information. Another is for measuring and comparing distances.

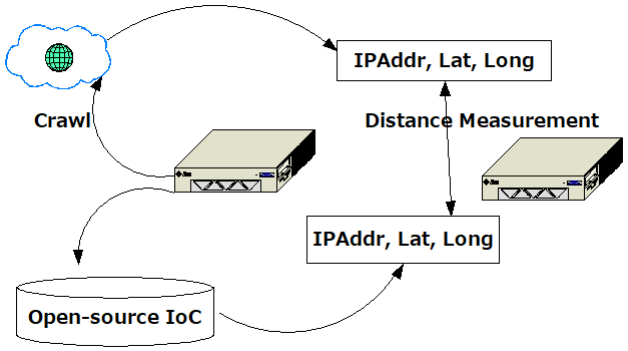


Figure 1: The flow chart of the proposed system

We have measured the list of distances between DNS and IP addresses in IoC. Algorithm 1 depicts the double loop to detect the shortest distance. The program executes a double loop from lines 1 to 9 to calculate the distance between 30,285,322 DNS servers and 294 hosts in IoC. In line 5, two distances measured are compared to find the minimum distance from IoC.

For handling 30,285,322 * 294 steps, we apply the data decomposition method for parallelizing the processing. Also, we use the python-multiprocessing module [19] for speeding up the parallel processing.

For calculating distance, we use GeoPy [7]. We wrote the code as follows:

```
from geopy.distance import geodesic

DNS = (X1, Y1)
IoC = (X2, Y2)

dis = geodesic(DNS, IoC).km
```

Algorithm 1 Detecting Nearest DNS server

Input: DNS, IoC
Output: Pair{IoC, nearest(DNS)}

```
while DNS server list do
  Min = 100000
  while IoC list do
    Dis = distance(DNS, IoC)
    if Dis < Min then
      Min = Dis
    end if
  end while
end while
```

GeoPy uses WGS84 (World Geodetic System 1984). By doing this, we can leverage the library of Python client for several popular geocoding web services.

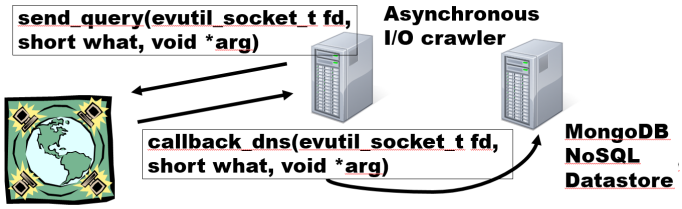


Figure 2: The overview of our system

4 Measurements

DNS is the most scalable ecosystem on the Internet. Also, the DNS is one of the most numerous Internet servers. For handling the response of thirty millions of DNS servers, we use scalable open source software of Libevent [8] and MongoDB [14].

Figure 2 depicts the overview of our system. We have divided our system into two servers: frontend crawling server and backend DB. On the frontend server shown in the middle of Figure 3, we employ Libevent for asynchromous event notification. DNS queries is issued in asynchronous I/O manner and capable for handling the response of which timeout cannot be estimated exactly. In experiment, it turned out that MySQL (or PostgreSQL) cannot handle about thirty millions of reponses in 26 hours. To hinder this problem, we use MongoDB which is document-based NoSQL datastore. MongoDB is scalabel and equip the utility useful in several situations in data processing such as aggregating, indexing and sorting with key-value data format. For example, we can easily implement prototyes for geospatial ananlysis and statistical analysis of software versions of DNS.

The procedures of our system is summarized as follows:

1) Asynchronous I/O crawler issues request by calling send_query.

2) callback_dns stores the response into MongoDB.

Note that (2) is activated in an asynchronous I/O manner.

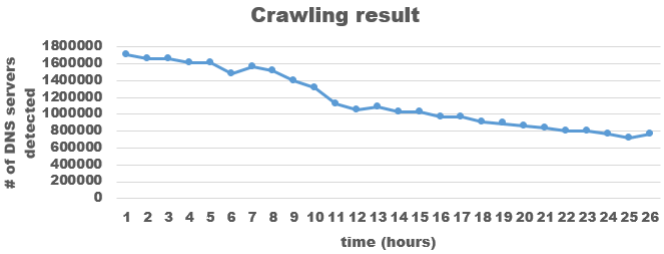


Figure 3: Crawling 30,285,322 DNS servers in 26 hours.

The purpose of the project in the first place was to detect the nearest DNS server geographically from each IP address of IoC. Then, two types of cases are presumed. The first one is that malicious host on IoC list abuses the DNS server. The second one is that the DNS server is compromised or malicious to be complicit with malicious hosts.

Libevent is an asynchronous mechanism to provide a callback function for handling specific events on a file or socket descriptor. Libvent also supports callbacks invoked by signals and regular timeouts. Libevent has three steps to achieve these procedures.

1) Setting struct event_base. The event_base is responsible for keeping track of which events are pending or active.

2) Event notification with struct event_new. Struct event_new is registered to the list to enable notification.

   The structure of the event is as follows:

3) Dispatching events. Activate event base loop by calling event_base_loop() for more fine-grained control.

```
struct event {
   struct event_callback ev_evcallback;
   evutil_socket_t ev_fd;
   struct event_base *ev_base;
}
```

This structure (struct event) has three members: socket descriptor, callback, and event base loop. In the implementation, we have embedded the driver of MongoDB to store the response received by the socket descriptor. We have succeeded in detecting about 30,000,000 DNS servers in reasonable crawling time (24 hours) [1].

In deployment, crawlers on the front end use Libevent, and the backend analyzer uses MongoDB. The Libevent-based crawler, which leverages asynchronous I/O on the NoSQL cluster, achieves high-speed active monitoring. We have succeeded in connecting 30,285,322 DNS servers in 26 hours.

5 Results

5.1 Distance Comparison between DNS and Traceroute

We have measured two kinds of distances of 304 IP addresses in IoC. One is from DNS server. Another is from ISP gateway. We use the traceroute utility to obtain the distance of ISP gateway.

Figure 4 shows the histogram of the two kinds of distance calculated about DNS and traceroute. The upper side of Figure 4 shows the number of DNS servers. We have observed that more than 50% of the servers are concentrated in the 400KM to 650KM value range. (see red area B). From this result, we have found that public DNS servers with global IP addresses have a wider range of operations (about 400-500KM) than we expected.

The lower side of Figure 4 shows the histogram of the ISP gateway detected by traceroute. More than 50% of gateway servers are located within 50KM from IP address in IoC (see area A). In this case, it is difficult to characterize DNS servers which are assumed to be the shortest from IP addresses in IoC. We should consider the situation where the DNS server is operating without the range of the nearest ISP gateway. In any event, information about area A can contributes to the further classification of IP addresses in IoC.

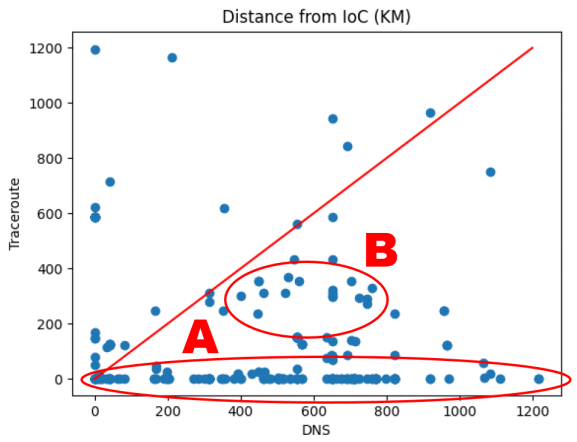


Figure 4: The histogram of the two kinds of distance calculated about DNS and traceroute

Figure 5 is a scatter diagram for the Comparison of DNS and gateway ISP. X-axis is the distance of DNS. Y-axis is the distance of the gateway ISP. We have marked two areas (A, B). Each area corresponds to the area A, and B of Figure 5.

We obtain two main findings as follows.

1) As far as observing A, there seems to be no correlation between the distance of DNS and gateway ISP. However, the range of distance of DNS servers is rising from 0 to 1200. It could be guessed that we have succeeded in detecting the nearest DNS servers in the left part of area A.
2) Area B has a cluster with the middle-range distance of DNS and gateway ISP. It could be guessed that the DNS server is located near the gateway ISP. In this case, ISP may operate both gateway DNS servers.

5.2 Usage Type of DNS

AbuseIPDB classifies IP addresses into 12 usage types based on the function of the organization/business unit. We can use usageType for filtering certain ranges of IP addresses for our needs. For example, if we are to check the IP address originates from a university, college, or school, we can check the EDU IP address.

1) Commercial
2) ContentDeliveryNetwork
3) DataCenterWebHostingTransit
4) FixedLineISP
5) Government
6) MobileISP
7) N.A.
8) SearchEngineSpider
9) UniversityCollegeSchool

We have generated a list of frequency of Usage type in both Grizzly Steppe and Hidden Cobra (sss Table 1).

We have generated a list of frequency of Usage type in both Grizzly Steppe and Hidden Cobra by issuing the one-linear as follows:

```
# cat $1 | jq -j '.data.ipAddress,","
,.data.usageType,"\n"
| tr -d "\/" | tr -d " "
 | sort | uniq ?c | sort -k 2,2
```

Our findings are as follows:

1) Many of DNS servers are located in Area B within the range of middle distance. The most common usage type of DNS servers in Area B is. From this point, it can be inferred that the DNS server administrator and the gateway ISP are different organizations.
2) Most of usage type in Area A (within 400km) is FixedLineISP. In Area B, DNS servers are located near the gateway ISP. In this aspect, it is guessed that Gateway ISP operates both DNS server and gateway in the same organization.
3) In Area C, usage type cannot be identified. We cannot know whether DNS administrator and gateway ISP are the same or not. Other survey items and features are needed to clarify the actual situation in Area C.

In any case, we can conclude that we can classify IoC further by the distance of DNS server.

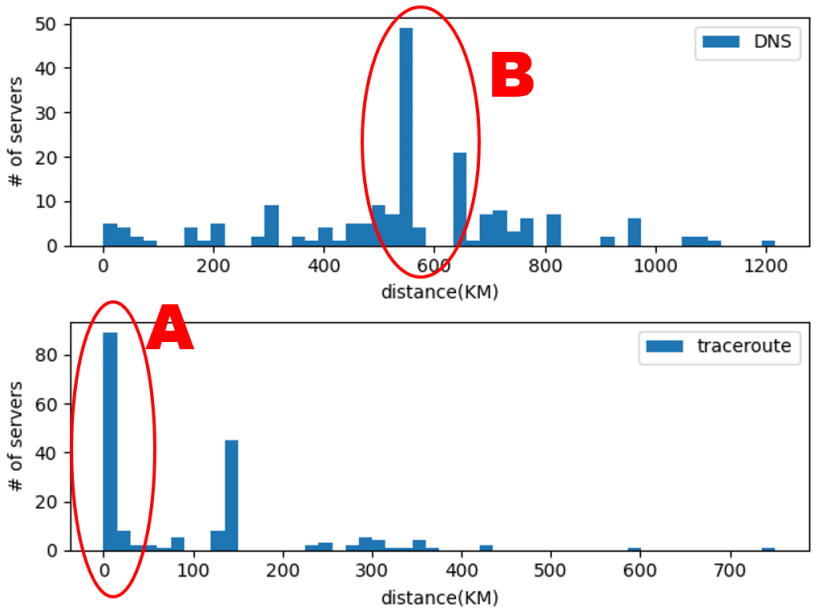


Figure 5: Comparison of the number of IP addresses of nearest ISP gateway and DNS. We have measured 294 IP addresses.

Table 1: Usage type of DNS servers

From 0 to 400 km (short)		
FixedLineISP	22	7.4 %
Commercial	20	6.8 %
null	18	6.1 %
DataCenter/WebHosting/Transit	18	6.1 %
ContentDeliveryNetwork		0.6 %
MobileISP	1	0.3 %
Total		79
From 400 to 800 km (middle)		
DataCenter/WebHosting/Transit	95	32.3 %
FixedLineISP	38	12.9 %
Commercial	20	6.8 %
null	10	3.4 %
Total		163
From 800 to 1250 km (long)		
null	16	5.4 %
DataCenter/WebHosting/Transit	8	2.7 %
FixedLineISP	4	1.3 %
Commercial	1	0.3 %
Total		29

6 Related Work

Pent *et al.* [18] present an evaluation of VirusTotal for phishing websites. They set up fake phishing websites by imitating PayPal and IRS. A data-driven engine for online analysis of malware are proposed by Zhu *et al.* [24]. They survey 115 academic papers and collected more than 14000 daily records of VirusTotal. Automated IP Reputation Analyzer Tool (AIPRA) based on some reliable blacklist databases was presented by Lewis *et al.* [12]. The Democratic National Committee's (DNC) operations in the past election season was reported by Karadi [11]. Malicious cyber activities of the Lazarus Group, a.k.a. Hidden Cobra was reported in [10]. Characterization of a type of reputation-based blacklist is discussed in Sinha *et al.* [20]. PhishFarm [15] analyzes 2,380 live phising site. Those are classified by 10 distinct anti-phishing entities.

An empirical assessment of commercial threat intelligence service of two leading vendors is performed by Bouwman *et al.* [4]. They interviewed 14 security professionals.

Zhao *et al.* [23] propose HINT1, which is a CTI framework for modeling the independent relationships among heterogeneous IoCs. Asiri *et al.* [2] presents the study of examining the effectiveness of the IOCs under an operational technology environment. Li *et al.* [13] propose a set of metrics to characterize threat intelligence data and apply it to a broad range of public and commercial sources.

Houser *et al.* [8] conduct an analysis of DNS hijacking based on passive DNS records and apply it to the DNS hijacking detection mechanism. Pearce *et al.* [17] present new patterns in DNS manipulations by Iris, which is a scalable method to measure global DNS resolutions. Liu *et al.* [14] perform a large-scale analysis of on-path DNS interception handled by recursive DNS servers. They leverage 148,378 residential and cellular IP addresses.

Augustin *et al.* [3] provide a traceroute for obtaining a more precise picture of routes, including graphs of loops, cycles, and diamonds. Huang *et al.* [9] propose a new traceroute implementation for large-scale topology discovery of the entire /24 address space.

In [3], a retroactive identification without fine-grained large-scale Internet data is propsed. They combines a

range of longitudinal data by Internet-wide scans, passive DNS records, and certificate transparency logs. In [21], they combine inferred DNS activity by a sizeable darknet with DNS measurement data for a 17 month period. Nawrocki *et al.* [21] evaluates the effectiveness of observed DNS attacks by traceing IXP-inferred attacks. Opara *et al.* [16] conducts a research of activities across the cyber security of medium and large farms.

7 Conclusions

In this paper, we perform a geospatial analysis of DNS servers to provide a more sophisticated IoC. We cope with the open IoC of Grizzly Steppe of Russian malicious cyber activity, which is released as an open-source IoC by US-CERT. First, we designed a rapid crawling system to find DNS servers, and we detected 30285322 DNS servers in 26 hours. Based on the list of IP addresses of DNS servers we detect, we have calculated the shortest distance from the IP address of IoC. As a result, we have detected the nearest DNS servers for each IP address of IoC. For 294 DNS servers we detect, we extract three groups by the distance. We extensively studied the characteristics of usageType of the DNS servers. We have found that we can classify DNS servers associated with IoC into three categories. Particularly, there are two distinguishing features.

1) At close range (within 400KM) where the most common usage type is FixedLineISP, DNS server is operated close to the gateway ISP.

2) At the middle range (ranging from 400KM to 600KM), where the most usage type is DataCenter/WebHosting/Transit , an administration of DNS server is different from one of gateway ISP.

For the three categories classified by distance, we have successfully found distinct characteristics by usage type. We apply our method for further classification of Russian malicious cyber activity called Grizzly Steppe. We believe that our analysis will be informative in generating a more sophisticated IoC.

References

[1] R. Ando, Y. Takano, S. Uda, "Unraveling large scale geographical distribution of vulnerable DNS servers using asynchronous I/O mechanism," in *Proceedings of The 2nd International Symposium on Grey-Hat Hacking*, pp. 116-129, 2013.

[2] M. Asiri, N. Saxena, P. Burnap, "Investigating Usable Indicators against Cyber-Attacks in Industrial Control Systems," *17th USENIX Symposium on Usable Privacy and Security (SOUPS'21)*, 2021.

[3] B. Augustin, X. Cuvellier, B. Orgogozo, F. Viger, T. Friedman, M. Latapy, C. Magnien, R. Teixeira, "Avoiding traceroute anomalies with Paris traceroute," *Internet Measurement Conference*, pp. 153-158, 2006.

[4] X. Bouwman, H. Griffioen, J. Egbers, C. Doerr, B. Klievink, M. van Eeten, "A different cup of TI? The added value of commercial threat intelligence," *USENIX Security Symposium*, pp. 433-450, 2020.

[5] Cybersecurity and Infrastructure Security Agency, *Russian Malicious Cyber Activity*, Apr. 16, 2018. (`https://www.cisa.gov/news-events/alerts/2018/04/16/russian-malicious-cyber-activity`)

[6] greenspun.com, *London Times— Russian Hack DoD computers*, Oct. 15, 2019. (`http://greenspun.com/bboard/q-and-a-fetch-msg.tcl?msg_id=0010lE`)

[7] GeoPy, *GeoPy's Documentation*, June 25, 2023. (`https://geopy.readthedocs.io/en/stable/`)

[8] R. Houser, S. Hao, Z. Li, D. Liu, C. Cotton, H. Wang, "A comprehensive measurement-based investigation of DNS hijacking," *SRDS*, pp. 210-221, 2021.

[9] Y. Huang, M. Rabinovich, R. Al-Dalky, "FlashRoute: Efficient Traceroute on a Massive Scale," *Internet Measurement Conference*, pp. 443-455, 2020.

[10] P. Kalnai, M. Poslusny, "Lazarus Group: A mahjong game played with different sets of tiles," *Virus Bulletin International Conference*, 2018.

[11] G. Karadi, *Russian Fingerprints on the DNC: OSINT FOR RUSSIAN INFILTRATION OF THE DNC*, 2017. (doi: 10.13140/RG.2.2.12549.60649)

[12] J. L. Lewis, G. F. Tambaliuc, H. S. Narman, W. S. Yoo, " IP Reputation Analysis of Public Databases and Machine Learning Techniques," in *ICNC*, pp.181-186, 2020.

[13] V. G. Li, M. Dunn, P. Pearce, D. McCoy, G. M. Voelker, S. Savage, "Reading the Tea leaves: A Comparative Analysis of Threat Intelligence," *USENIX Security Symposium*, pp. 851-867, 2019.

[14] B. Liu, C. Lu, H. X. Duan, Y. Liu, Z. Li, S. Hao, M. Yang, "Who is answering my queries: understanding and characterizing interception of the DNS resolution path," in *Proceedings of the Applied Networking Research Workshop (ANRW'19)*, pp. 15-16, 2019.

[15] A. Oest, Y. Safaei, A. Doup, G. J. Ahn, B. Wardman, K. Tyers, "PhishFarm: A Scalable Framework for Measuring the Effectiveness of Evasion Techniques against Browser Phishing Blacklists," *IEEE Symposium on Security and Privacy*, pp. 1344-1361, 2019.

[16] E. U. Opara, O. J. Dieli, "Enterprise cyber security challenges to medium and large firms: An analysis," *International Journal of Electronics and Information Engineering*, vol. 13, no. 2, pp. 77-85, 2021.

[17] P. Pearce, B. Jones, F. Li, R. Ensafi, N. Feamster, N. Weaver, V. Paxson, "Global Measurement of DNS Manipulation," *USENIX Security Symposium*, pp. 307-323, 2017.

[18] P. Peng, L. Yang, L. Song, G. Wang, "Opening the blackbox of virustotal: Analyzing online phishing scan engines," *Internet Measurement Conference*, pp.478-485, 2019.

[19] Python, *multiprocessing — Process-based Parallelism*, Apr. 16, 2023. (`https://docs.python.org/3/library/multiprocessing.html`)

[20] S. Sinha, M. Bailey, F. Jahanian, "Shades of grey: On the effectiveness of reputation-based blacklists," *Malware*, pp. 57-64, 2008.

[21] R. Sommese, K. C. Claffy, R. van Rijswijk-Deij, A. Chattopadhyay, A. Dainotti, A. Sperotto, M. Jonker, "Investigating the impact of DDoS attacks on DNS infrastructure," in *Proceedings of the 22nd ACM Internet Measurement Conference (IMC'22)*, pp. 51-64, 2022.

[22] J. R. Sun, M. S. Hwang, "A new investigation approach for tracing source IP in DDoS attack from proxy server", in *Intelligent Systems and Applications*, pp. 850-857, 2015.

[23] J. Zhao, Q. Yan, X. Liu, B. Li, G. Zuo, "Cyber Threat Intelligence Modeling Based on Heterogeneous Graph Convolutional Network," *RAID*, pp. 241-256, 2020.

[24] S. Zhu, J. Shi, L. Yang, B. Qin, Z. Zhang, L. Song, G. Wang, "Measuring and modeling the label dynamics of online anti-malware engines," *USENIX Security Symposium*, pp.2361-2378, 2020.

Biography

Ruo Ando received Ph.D. from Keio University in 2006. He is now associate professor by special appointment of National Institute of Informatics since 2016. Before joining NII, he worked as senior researcher of National Institute of Information and Communications Technology since 2006. His research interests focus on network security, information security and big data mining technologies.He received Outstanding Leadership Award in the 8th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC-09) at China in 2009. He is the member of Trusted Computing Group JRF (Japan Regional Forum) in 2008-2015. He worked in project "Next Generation Security Info-Security R&D" METI (FY2008-10). He was engaged in project "Unknown malware detection using incremental malware detection" MEXT FY(2012-2015).

Hiroshi Itoh received the Master degrees from Keio University in 1980. He has Doctor of engineering from Keio University. He is now Executive Researcher in National Institute of Information and Communications Technology in Japan. He was working in Symantec Japan, Inc. from 2007 to 2010. He was Deputy Director-General for Cybersecurity and Information Technology Management in Ministry of Economy, Trade and Industry.

RBAC-based Delegation Authorization with Trust Computing and Collaborative Security Strategy

Wei Sun

(Corresponding author: Wei Sun)

School of Computer and Information Technology, Xinyang Normal University
No. 237, Nanhu Road, Xinyang 464000, P. R. China
Email: sunny810715@xynu.edu.cn

(Received Feb. 4, 2023; Revised and Accepted June 4, 2023; First Online June 25, 2023)

Abstract

Role-based access control (RBAC) is very popular as it has various security-control strategies and provides a flexible authorization mechanism. Delegation authorization based on RBAC is an effective method that decentralizes the authorization management from the delegating subject to the delegated object. However, delegations are arbitrary using the existing approaches, particularly in large-scale distributed and collaborative systems. The delegation process becomes unreliable once the delegated object with lower trustworthiness is selected, and the security of the system status cannot be guaranteed. Aiming at these issues, this study proposes a novel delegation method based on the trust relationship and the collaborative security strategy and then presents its delegation-authorization process. First, to reflect the reliability of the delegation process, the trust degrees of different candidate objects are comprehensively calculated using the trust seniority, trust experience, and trust recommendation, and the delegated objects with higher values are selected. Second, to ensure system security, the collaborative division of duties is introduced, which can be implicitly enforced by the mutually exclusive-role constraints to determine further the most appropriate delegated object in the secure collaborative environment. The experimental results show that, compared to the existing studies, the proposed method effectively improves the reliability of the delegation process and satisfies the various security requirements of organizations.

Keywords: Collaborative Security Strategy; Mutually Exclusive Constraint; Role-based Access Control; Trust Relationship

1 Introduction

The role-based access control (RBAC), owing to the characteristic of the convenience for authorizations as well as its various security policies, had emerged as a very popular mechanism and had been widely adopted by the organizations of all scales over the past few decades [6, 8, 21]. As an important manifestation of the RBAC system, the delegation-authorization technique based on RBAC chooses an appropriate delegated object as the substitute for the delegating subject or user, in order to decentralize the centralized authorization management to some ordinary object. The delegation authorization has been proved to be flexible and useful in many practical applications [3, 4, 16]. With the high-speed advance and wide application of the emerging network-information technologies, including the Internet of Things (IoT), edge computing and blockchain, the security and reliability of the information system are regarded as two increasing prominent problems, which have been attracting much attention in both academia and industry in recent years.

In the computer-supported distributed and collaborative working systems, multiple users are required to cooperate and communicate with each other, in order to jointly make the access decision to information resources, while achieving the purpose of the mutual restrictions [1, 22, 24]. As an effective access-control strategy, the trust-collaboration mechanism meets the confidentiality and privacy requirements of information resources, and it reduces the possibility of abusing authorities due to the randomness of the delegation. Therefore, when some user is temporarily absent or on leave, how to develop a reliable and secure delegation scheme for choosing a trustworthy substitute to participate in the collaboration is very challenging.

In light of the above-mentioned problems, this study proposes a novel method, called RBAC-based delegation

authorization with the trust computing and collaborative security strategy (RDA_TC&CSS), and then presents its process in detail. The main contributions of this work are as follows:

1) To improve the reliability of the delegation process, we employ the trust relationship, including the trust seniority, trust experience and trust recommendation to comprehensively compute the trust degrees of different candidate objects, and then choose the objects with higher values. We demonstrate the effectiveness of the RDA_TC&CSS using a specific simulated system.

2) To ensure the system security, while avoiding the abuse of authorities due to the randomness of delegations, we utilize the collaborative security strategy to further determine the most appropriate delegated object in the specific collaborative scenario, and then indirectly implement the strategy by constructing the mutually-exclusive-role constraints. We demonstrate the efficiency of the RDA_TC&CSS using real-world datasets.

The rest of the article is structured as follows. We discuss some related work in Section 2. Section 3 introduces the necessary preliminaries used for our work. Section 4 proposes a novel delegation method and presents its delegation-authorization process. We present the experimental analysis in Section 5 and conclude the article and discuss future work in Section 6.

2 Related Work

Aiming at the problems of the heavy management burden and lack of the flexibility for the centralized authorization, Crampton *et al.* [7] proposed the RBAC-based delegation to flexibly transfer the authorization management to ordinary users, which alleviates the burden of the system management and has some reference for studying the delegation in the collaborative environment. Alsulaiman *et al.* [5] proposed a threshold-based collaborative access control model, called TBCACM, which associates the access privileges of the resources with the threshold, transfers permissions with the contribution coefficients to the delegated users to participate in collaboration and makes common decision for accessing resources. Yu *et al.* [23] proposed a locale-based access control model (LCACM) in the collaborative environment and presented a hierarchical authorization mechanism within the collaborative group, which could meet the security and flexibility requirements of the delegation. Khan *et al.* [9] proposed a security delegation model by restricting the delegation of sensitive permission as well as restriction from unauthorized access to resources, which could reduce the administrative burden and enable the automated delegation. Actually, the delegating subject should select competent and trustworthy delegated objects from many candidate objects with different degrees of trust and execution. However, there exists the problem of arbitrariness in most of the existing approaches. The delegation process becomes unreliable once the delegated object with lower trustworthiness is selected.

To realize the fine-grained, accurate and reliable delegation authorization, Liu *et al.* [13] combined conventional RBAC model and trust management and proposed a trust-based access control model (TBACM), which comprehensively calculated the trust degrees of different users and evaluated their behavior ability. According to the dynamic changes of user behavior, Zhu [25] divided the user trust into static trust level and dynamic trust level and proposed a user trust-based dynamic multi-level access control model (UTDMACM), which could realize the hierarchical access control and fine-grained dynamic authorization. According to the dynamic variability of the network environment and user status, Liu and Chang [12] introduced the concept of trust measure and context constraint and proposed a novel access control model based on the multi-dimension measurement and context, called MMCBACM, which could realize the dynamic and real-time control to the delegation authorization. To mitigate the malicious actions caused by the authenticated users, Abdul *et al.* [2] designed an access control mechanism by computing the trust degree based on the user's uncertain behavior, which could accurately detect and mitigate malicious users from the mobile cloud computing environment. These models or mechanisms can better reflect the reliability of the delegation process. However, they cannot meet the security requirements for a given collaborative working environment, and there may be potential security risks.

A key characteristic of RBAC is that it allows the specification and enforcement of various constraint policies [10, 15], such as the cardinality constraint and separation-of-duty constraint (SOD). As a significant constraint strategy discussed in this study, the SOD states that at least k users are required to complete a special task that requires n permissions, while any $(k-1)$ users are not allowed to together have all these permissions needed to complete the task [17]. It has been regarded as a critical principle of the information-system security and is widely used in large-scale distributed and collaborative systems. Sarana *et al.* [18] proposed a novel role-optimization method represented as RMP_SoD when the SOD constraints were present and developed three alternative approaches either during or after the role mining. In order to satisfy SOD constraints while ensuring authorization security, Sun *et al.* [20] proposed a role-mining method, called role-mining optimization with separation-of-duty constraints and security detection for authorizations (RMO_SODSDA). Subsequently, Sun *et al.* [19] proposed another novel policy-engineering method, called policy-engineering optimization with visual representation and separation of duty constraints (PEO_VR&SOD), which utilized the method of SAT-based model counting to reduce the constraints and constructed mutually exclusive constraints, in order to implicitly enforce the given

SOD constraints. In the above-mentioned approaches for constructing RBAC systems with the SOD constraints, however, an inadequately addressed key challenge is that occurrence of the delegation cases is not taken into consideration.

3 Preliminaries

Before proposing our methodology, some preliminaries are presented, including the trust relationship and collaborative security strategy.

3.1 Trust Relationship

The trust relationship between the delegating subject and the delegated object, referring to the literature [2], lies on three factors: the trust seniority, trust experience and trust recommendation. Specifically, the trust seniority indicates the inherent properties of the delegated object, including the basic seniority of the object itself and the affiliated seniority of the associated roles; the trust experience indicates the effect of the candidate object having completed the task on behalf of the delegator in the past; The trust recommendation indicates the trust evaluation of the third party for the candidate object. For convenience, both the subjects and objects represent persons in the following.

1) Task attribute ta_i: Multiple users $u_1, u_2, \cdots$ must have a series of qualification conditions $a_{i_1}, a_{i_2}, \cdots, a_{i_n}$ required by task t_i, before they are cooperating to perform t_i. The combinational set of $a_{i_1}, a_{i_2}, \cdots, a_{i_n}$ is regarded as the task attribute of t_i, denoted as $ta_i = \{a_{i_1}, a_{i_2}, \cdots, a_{i_n}\}$.

2) User attribute ua_j: Collaborative user u_j owns a series of qualification conditions $a_{j_1}, a_{j_2}, \cdots, a_{j_m}$, which are regarded as the user attribute, denoted as $ua_j = \{a_{j_1}, a_{j_2}, \cdots, a_{j_m}\}$.

3) Basic seniority $A_{j\to i}$: It is used to represent the basic seniority of user u_j with respect to task t_i. Assuming the weight values $wa_{i_1}, wa_{i_2}, \cdots, wa_{i_n}$ respectively represent the importance of $a_{i_1}, a_{i_2}, \cdots, a_{i_n}$ towards task t_i, where $0 \le wa_{i_r} \le 1$, and $\sum_{r=1}^{n} wa_{i_r} = 1$. Then $A_{j\to i} = \sum_{k=1}^{p} wa_{i_k}$, where $p \le |ua_j \cap ta_i—$, wa_{i_k} is the weight associated to a_{i_k}, and $a_{i_k} \in ua_j \cap ta_i$.

4) Affiliated seniority $RA_{j\to i}$: User u_d needs to delegate his authorities to another user u_j through role r_d, when u_d collaboratively participates in performing task t_i. If $dist(r_d, r_j)$ indicates the distance between r_d and r_j on the same role hierarchy RH, where $0 \le dist(r_d, r_j) \le 1$, then $dist(r_d, r_j)$ is regarded as the affiliated seniority of u_j with respect to t_i, denoted as $RA_{j\to i} = dist(r_d, r_j)$. Obviously, the greater the value of $RA_{j\to i}$, the closer connection between u_j and u_d is. If r_d and r_j are not on the same role hierarchy, then u_j and u_d have no connection, that is $RA_{j\to i} = 0$.

5) Trust seniority $P_{j\to i}$: The basic seniority $A_{j\to i}$ and the affiliated one $RA_{j\to i}$ together constitute the trust seniority, denoted as $P_{j\to i} = w_a \times A_{j\to i} + w_{ra} \times RA_{j\to i}$, where w_a, and w_{ra} respectively represent the contributions of $A_{j\to i}$ and $RA_{j\to i}$ for $P_{j\to i}$, $0 \le w_a, w_{ra} \le 1$, and $w_a + w_{ra} = 1$.

6) Trust experience $E_{j\to i}$: As a substitute for the delegating user u_d, the delegated user u_j has participated in the process of performing task t_i a few times in the past. The total effect of u_j completing the task is regarded as the trust experience, denoted as $E_{j\to i} = \sum_(k = 1)^n wt_{j_k} \times e_{j_k}$, where $wt_{j_k} = k/n$ $(1 \le k \le n)$ is used to represent the empirical coefficient of u_j in the k-th execution of t_i, and the more recent the execution time, the greater value of wt_{j_k} is; e_{j_k} is used to represent the effect of the k-th completing the task, $0 \le e_{j_k} \le 1$, which can be stated as follows:

$$e_{j_k} = \begin{cases} = 1 & \text{successful execution} \\ = 0 & \text{false execution} \\ \longrightarrow 1 & \text{performing well} \\ \longrightarrow 0 & \text{performing poor} \end{cases} \quad (1)$$

7) Trust recommendation $R_{j\to i}$: When u_d needs to delegate his authorities to u_j through the joint recommendation of m users $ur_1, ur_2, \cdots, ur_m$, the trust recommendation of u_j with respect to the task is denoted as: $R_{j\to i} = \frac{\sum_{k=1}^{m} t_k \times r_{k_j}}{\sum_{k=1}^{m} t_k}$, where $t_k (1 \le k \le m)$ is used to represent the trust value of the system to ur_k, rk_j represents the recommendation value of ur_k to u_j, and $0 \le t_k, r_{k_j} \le 1$.

3.2 Collaborative Security Strategy

The collaborative security strategy, including the collaborative division of duties and the mutually-exclusive-role constraints, can ensure the security and satisfiability of the system status. Similar to the well-known SOD principle, the collaborative division of duties is a common security strategy in the multi-user cooperative scenarios, which can be effectively enforced by the mechanism of the mutually-exclusive-role constraint [20]. For the sake of brevity, we assume that any role associates with only one permission.

1) System status γ: It is formalized as a triple $< UA, PA, RH >$, denoted as γ, where UA, PA and RH are the basic components of the RBAC model. $Roles_\gamma(u)$, and $Perms_\gamma(u)$ represent the roles and the permissions assigned to u under γ, respectively,

which are formalized as follows:

$$\begin{aligned} Roles_\gamma(u) &= \{r \in R | \exists r_1 \in R, \\ &\quad (u, r_1) \in UA \wedge (r_1, r) \in RH\}; \\ Perms_\gamma(u) &= \{p \in P | \exists r_2 \in R, \\ &\quad (p, r_2) \in PA \wedge (Roles_\gamma(u), r_2) \in RH\}. \end{aligned}$$

2) Collaborative division of duties $k-n$ CDOD: It states that at least k users are required to cooperate with each other, in order to together execute a specific task involving n roles and have all these roles, which can be expressed as $e = cdod < \{r_1, r_2, \cdots, r_n\}, k >$, where $1 < k \leq n$.

3) Static mutually-exclusive-role constraint t-m SMER: It states that any user cannot have t or more roles out of the given m roles, which can be expressed as $c = smer < \{r_1, r_2, \cdots, r_m\}, t >$, where $1 < t \leq m$. When $t = m$, it is also denoted as the $t - t$ SMER, which is more restricted than the $t - m$ SMER.

4) Security of the system status $sec(\gamma)$: Given a $k - n$ CDOD $e = cdod < \{r_1, r_2, \cdots, r_n\}, k >$ under the system status γ, if any $(k-1)$ users cannot have all these n roles under γ, then γ is secure, denoted as $sec_e(\gamma) = 1$; otherwise, γ is not secure, denoted as $sec_e(\gamma) = 0$. Let the set of variants of $k-n$ CDOD be $E = \{e_1, e_2, \cdots\}$, if γ is secure with respect to each e_i, then γ is secure with respect to E; otherwise, γ is not secure with respect to E. Whether or not the system status is secure can be formalized as follows:

$$\begin{aligned} \forall e \in E, \exists \{u_1, u_2, \cdots, u_{k-1}\} \subset U : \\ \{r_1, r_2, \cdots, r_n\} \nsubseteq \bigcup_{i=1}^{k-1} Roles_\gamma(u_i) \\ \Rightarrow sec_e(\gamma) = 1; \\ \exists e \in E, \exists \{u_1, u_2, \cdots, u_{k-1}\} \subset U : \\ \bigcup_{i=1}^{k-1} Roles_\gamma(u_i) \supseteq \{r_1, r_2, \cdots, r_n\} \\ \Rightarrow sec_e(\gamma) = 0. \end{aligned}$$

5) Satisfiability of the system status $sat(\gamma)$: Given a $t - m$ SMER $c = smer < \{r_1, r_2, \cdots, r_m\}, t >$ under the system status γ, if no user is allowed to have t or more roles out of all these m roles under γ, then γ is satisfied, denoted as $satc(\gamma) = 1$; otherwise, γ is not satisfied, denoted as $satc(\gamma) = 0$. Let the set of variants of $t - m$ SMER be $C = \{c_1, c_2, \cdots\}$, if γ is satisfied with respect to each ci, then γ is satisfied with respect to C; otherwise, γ is not satisfied with respect to C. Whether or not the system status is satisfied can be formalized as follows:

$$\begin{aligned} \forall c \in C, \exists u \in U : \\ |Roles_\gamma(u) \cap \{r_1, r_2, \cdots, r_m\}| < t \\ \Rightarrow sat_c(\gamma) = 1; \\ \exists c \in C, \exists u \in U : \\ |Roles_\gamma(u) \cap \{r_1, r_2, \cdots, r_m\}| \geq t \\ \Rightarrow sat_c(\gamma) = 0. \end{aligned}$$

4 Methodology

In this section, based on the trust relationship and collaborative security strategy, the framework of the proposed RDA_TC&CSS is presented as shown in Figure 1. It involves two main aspects: The delegation-authorization flows, and the connected components for the strategy deployment. First, definitions for the calculation of trust degree and the implicit enforcement of security strategy are presented as follows.

Definition 1. *Trust degree $T_{j\to i}$. The trust seniority $P_{j\to i}$, experience $E_{j\to i}$ and recommendation $R_{j\to i}$ together constitute the trust degree of u_j with respect to t_i, which can be calculated and expressed as $T_{j\to i} = w_p \times P_{j\to i} + w_e \times E_{j\to i} + w_r \times R_{j\to i}$, where w_p, we and w_r respectively represent the contribution coefficients of $P_{j\to i}$, $E_{j\to i}$ and $R_{j\to i}$ for $T_{j\to i}$, $0 \leq w_p, w_e, w_r \leq 1$, and $w_p + w_e + w_r = 1$.*

For the specific trust threshold $H_{j\to i}$ in the system, if $T_{j\to i} \geq H_{j\to i}$, then the candidate u_j is trustworthy; otherwise, u_j is not trustworthy.

According to Items (4) and (5) in Subsection 3.2, given the $k - n$ CDOD set E and $t - m$ SMER set C under the system status γ, the process of verifying whether or not γ is secure is in P; similarly, the process of verifying whether or not γ is satisfied is also in P. These two statements have been discussed in other related research, and then the enforcement condition of the secure strategy is presented, in order to determine the relationship between the $k - n$ CDOD and $t - m$ SMER.

Definition 2. *Implicit enforcement of the. $k-n$ CDOD. For the given collaborative strategy e and a constraint set C under γ, e can be implicitly enforced by C, if and only if $\forall c \in C : sat_c(\gamma) \Rightarrow sec_e(\gamma)$.*

4.1 Basic Components for the Strategy Deployment

The deployment for the RDA_TC&CSS mainly consists of the following four connected components:

1) Policy information point (PIP) is responsible for collecting and classifying the information records such as the user attributes, role attributes, historical interactions and user evaluations stored in database DB2, and then it effectively computes the trust relationship.

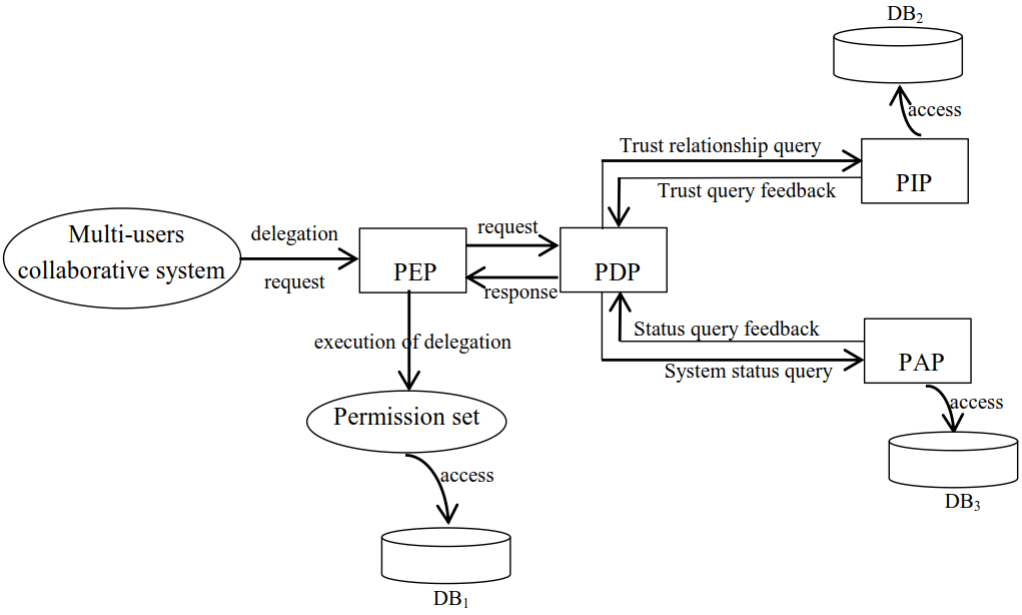


Figure 1: Framework of the RDA_TC&CSS

2) Policy administration point (PAP) is responsible for collecting and classifying the information records such as the collaborative division of duties and the mutually exclusive constraints stored in database DB3, and then it effectively analyzes the security and satisfiability requirements of the system status.

3) Policy decision point (PDP) is responsible for sending the query requests of the trust relationship and system status to PIP and PAP, respectively. It also makes the decision judgment and feeds it back to PEP according to the results of the trust computing and status analysis.

4) Policy enforcement point (PEP) is responsible for receiving the delegation request instructions from users. It also performs the delegation operation according to the decision feedback by the PDP and transfers the corresponding authorities of the delegating users stored in database DB1 to other users.

4.2 Process of the Delegation Authorization

To reflect the reliability of the delegation process and ensure the system security, the detailed procedure of the delegation authorization is presented as follows:

Step 1. In the working environment with collaborative execution of task t_i, user ud sends a delegation request instruction to PEP.

Step 2. PEP sends the request message to PDP and waits for PDP to make a decision response.

Step 3. PDP sends the query request of trust relationship to PIP, and PIP comprehensively calculates the trust degrees of candidate users $\{u_1, u_2, \cdots\}$ according to the records of user attributes, role attributes, historical interactions and user evaluations.

Step 4. Comparing the trust degree $T_{j\to i}$ of the candidate object u_j with the threshold $T_{j\to i}$ set in advance. If $T_{j\to i} \geq H_{j\to i}$, then u_j is inserted into the trustworthy object set and the procedure turns to Step 7; otherwise, u_j is moved from $\{u_1, u_2, \cdots\}$ and the procedure turns to Step 3.

Step 5. PDP sends the query request of system status to PAP, and PAP analyzes and presents the security and satisfiability requirements of the system status, according to records of the collaborative division of duties $\{e_1, e_2, \cdots\}$ and mutually exclusive constraints $\{c_1, c_2, \cdots\}$.

Step 6. Determining whether any e_l in $\{e_1, e_2, \cdots\}$ can be implicitly enforced by some subset of $\{c_1, c_2, \cdots\}$. If c_k can enforce e_l and it belongs to set C by constraint-construction method, then c_k is regarded as the minimal constraint; otherwise, c_k is moved from $\{c_1, c_2, \cdots\}$ and the procedure turns to Step 5.

Step 7. The result of the trust query in Step 4 and that of the status query in Step 6 are fed back to PDP, respectively.

Step 8. The trustworthy candidate objects are comprehensively investigated by PDP, in order to choose the most appropriate as the delegated user, such as u_j. Further, if u_j meets all the constraint requirements, then the decision result "allow delegation" is fed back to PEP; otherwise, u_j is moved from the candidates and other objects are reviewed.

Step 9. PEP executes the delegation-authorization operation on u_j.

4.3 Construction of the SMER Constraints

To implicitly enforce $k-n$ CDOD, we present an approach for constructing $t-m$ SMER constraints from the $k-n$ CDOD as shown in Algorithm 1. It is observed from Lines 2–5 of the algorithm that, the following statement is determined first.

Algorithm 1 Construction of $t-m$ SMER constraints

1: **Input:** $k-n$ CDOD constraint $cdod =< \{r_1, r_2, \cdots, r_n\}, k >$, where $1 < k \leq n$
2: **Output:** set C of $t-m$ SMER constraints
3: Initialize $C = \phi$;
4: **if** $k = 2$ **then**
5: $C = \{< \{r_1, r_2, \cdots, r_n\}, n >\}$;
6: **else if** $k = n$ **then**
7: $C = \{< \{r_1, r_2, \cdots, r_n\}, 2 >\}$;
8: **else**
9: **for** $(t = 2; \lfloor \frac{n-1}{k-1} \rfloor + 1; t++)$ **do**
10: $m = (k-1) \times (t-1) + 1$;
11: **for** any subset $\{r_1, r_2, \cdots, r'_m\}$ in $\{r_1, r_2, \cdots, r_n\}$ **do**
12: $C = C \cup \{< \{r_1, r_2, \cdots, r'_m\}, t >\}$;
13: **end for**
14: **end for**
15: **end if**

Statement 1. *For the given collaborative strategy $e = cdod < \{r_1, r_2, \cdots, r_n\}, k >$ under status γ, it can be precisely enforced by the constraint formalized as $c = smer < \{r_1, r_2, \cdots, r_n\}, t >$, if and only if $t = 2$ when $k = n$ (or $t = n$ when $k = 2$).*

Theorem 1. *For the given collaborative strategy $e = cdod < \{r_1, r_2, \cdots, r_n\}, k >$ under status γ , the SMER constraint set constructed by Algorithm 1 is minimal.*

Proof.
According to Statement 1, $\{< \{r_1, r_2, \cdots, r_n\}, 2 >\}$ and $\{< \{r_1, r_2, \cdots, r_n\}, n >\}$ is the minimal set required. Next, w_e need to verify whether if holds true when $2 < k < n$. The verification process considers the following two sides.

On one hand, Any $(k-1)$ users have $(k-1) \times (t-1)$ roles from $\{r_1, r_2, \cdots, r_m\}$ at most, since any user at most is allowed to have $(t-1)$ roles. Without loss of generality, let t takes the value $(\lfloor \frac{n-1}{k-1} \rfloor + 1)$, the number of roles covered by any $(k-1)$ users is: $(k-1) \times (\lfloor \frac{n-1}{k-1} \rfloor + 1 - 1) < n$, that is $sat_c(\gamma) \Rightarrow safe_e(\gamma) = 1$. When $t < (\lfloor \frac{n-1}{k-1} \rfloor + 1)$, it also holds true. Thus, for each $c = smer < \{r_1, r_2, \cdots, r_m\}, t >$ in the constructed C, c can enforce e.

On the other hand, the contradiction method is used. Assuming that c is not the minimal constraint to enforce e, and there exists another enforceable $t' - m'$ SMER c' that is less strict than c, then m' should not be greater than m, and t' should be greater than t. There are two cases:

1) When $m' = m$ and $t' > t$, the assumption is true. Then, it is concluded that $t' > \lfloor \frac{n-1}{k-1} \rfloor + 1$. Without loss of generality, let t takes the value $(\lfloor \frac{n-1}{k-1} \rfloor + 2)$. For c', there exists $(k-1)$ users and the number of roles covered by these users is: $(k-1) \times (\frac{n-1}{k-1} + 2 - 1) = n - 1 + k - 1 > n$, then $sec_e(\gamma) = 0$, which breaches e. Thus, the assumption is false.

2) When $m' < m$ and $t' = t$, the assumption is true. If $sat_{c'}(\gamma) = 1$, then $sat_c(\gamma) = 1$, which indicates that c' that is not weaker than c. Thus, the assumption is false and the theorem is proved.

□

5 Experimental Analysis

To evaluate the performance of the RDA_TC&CSS, we next conduct experiments using the simulated system and real-world datasets, in order to demonstrate the reliability and security of the proposal. All the experiments are compiled and run under the Java environment.

5.1 Performance Evaluations for Reliability of the RDA_TC&CSS

5.1.1 Problem Statement

In the following simulated system, Figure 2 presents the role-hierarchy relationship (RH) of the RBAC system when a specified organization is purchasing a batch of products. Table 1 and Table 2 represent the relationship of the original user–role assignments (UA), and that of the original role–permission assignments (PA) in the multi-department collaborative working environment, respectively. If the assistant manager c is on a business trip and he needs to temporarily delegate his authorities to another collaborator, such as the assistant manager e, inspector g, or storing man h, in order to execute the corresponding tasks as the substitute of c, then the analysis for the delegation authorization is as follows.

5.1.2 Trust Computing

If the correspondence between the task attribute $t_{S\_DM_2}$ = {manager level, warehouse storage} and weight is: $wa_{\text{manager level}} = 0.6$, $wa_{\text{warehouse storage}} = 0.4$, then the basic seniorities of e, g, and h for $t_{S\_DM_2}$ are $A_{e \to t_{S\_DM_2}} = 0.6$, $A_{g \to t_{S\_DM_2}} = 0.4$, and $A_{h \to t_{S\_DM_2}} = 0.4$, respectively. Moreover, it is seen from Figure 2 that, S_DM_2, QP, and WP are on the same branch, while S_DM_2 and A_DM belong to different branches. If $dist(S\_DM_2, QP) = dist(S\_DM_2, WP) =$

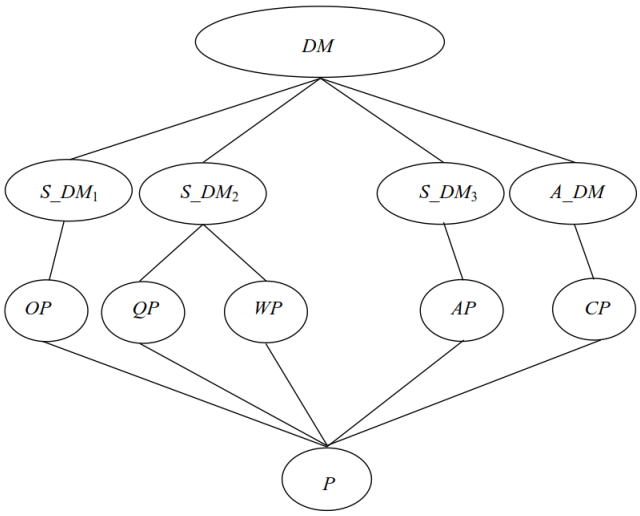


Figure 2: RH

Table 2: PA

Role	Permission	Annotation for permission
DM	p_1	It is responsible for general management
S_DM_1	p_2	It is responsible for ordering products
S_DM_2	p_3	It is responsible for keeping the warehouse
S_DM_3	p_4	It is responsible for financial accounting
A_DM	p_5	It is responsible for cash accounting
OP	p_6	Order products
QP	p_7	Inspect the product quality
WP	p_8	Store products
AP	p_9	keep accounts
CP	p_{10}	Revenue and expenditure cash
P	p_{11}	Collect and organize documents

Table 1: UA

User	Role	Annotation for role
a	DM	Department manager
b	S_DM_1	Assistant manager
c	S_DM_2	Assistant manager
d	S_DM_3	Assistant manager
e	A_DM	Assistant manager
f	OP	Ordering person
g	QP	Inspector
h	WP	Store keeper
i	AP	Accountant
j	CP	Cashier
k	P	Common staff

0.7, $dist(S\_DM_2, A\_DM) = 0$, then the affiliated seniorities of e, g, and h for $t_{S\_DM_2}$ are $RA_{e\to t_{S\_DM_2}} = 0$, $A_{g\to t_{S\_DM_2}} = 0.7$, and $A_{h\to t_{S\_DM_2}} = 0.7$, respectively.

If the basic seniority and affiliated seniority have the same contribution weight, then the trust seniorities of e, g, and h for $t_{S\_DM_2}$ are respectively calculated as:

$$\begin{aligned} P_{e\to t_{S\_DM_2}} &= w_a \times A_{e\to t_{S\_DM_2}} + w_{ra} \times RA_{e\to t_{S\_DM_2}} \\ &= 0.5 \times 0.6 + 0.5 \times 0 \\ &= 0.30 \\ P_{g\to t_{S\_DM_2}} &= w_a \times A_{g\to t_{S\_DM_2}} + w_{ra} \times RA_{g\to t_{S\_DM_2}} \\ &= 0.5 \times 0.4 + 0.5 \times 0.7 \\ &= 0.55 \\ P_{h\to t_{S\_DM_2}} &= w_a \times A_{h\to t_{S\_DM_2}} + w_{ra} \times RA_{h\to t_{S\_DM_2}} \\ &= 0.5 \times 0.4 + 0.5 \times 0.7 \\ &= 0.55 \end{aligned}$$

Taking the "year" as the measurement unit, the performances of e, g, and h in place of c in the last 5 years are investigated, respectively. Table 3 presents the completion effects with respect to the measurement unit and empirical coefficient, where "\" represents unknown. Providing that e, g, and h have the same empirical coefficient in the same unit of measurement. According to the table, the trust experiences of e, g, and h for $t_{S\_DM_2}$ are

respectively calculated as follows:

$$\begin{aligned} E_{e\to t_{S\_DM_2}} &= \sum_{k=1}^{5} wt_k \times e_{ek} \\ &= 0+0+0+0+1.0\times 0.8 \\ &= 0.80 \\ E_{g\to t_{S\_DM_2}} &= \sum_{k=1}^{5} wt_k \times e_{gk} \\ &= 0+0.4\times 0.6+0+0.8\times 0.4+0 \\ &= 0.56 \\ E_{h\to t_{S\_DM_2}} &= \sum_{k=1}^{5} wt_k \times e_{hk} \\ &= 0.2\times 0.7+0+0.6\times 0.5+0+0 \\ &= 0.44 \end{aligned}$$

In the existing collaboration environment, consider that the manager a, assistant managers b and d are selected as the referees of e, g, and h, respectively. Owing to the rank of a being above b, and d, the trust value of the system about the referee should be: $t_a > t_b$, and $t_a > t_d$. Table 4 presents the trust recommendations with respect to different referees. According to the table, the trust experiences of e, g, and h for $t_{S\_DM_2}$ are respectively calculated as follows:

$$\begin{aligned} R_{e\to t_{S\_DM_2}} &= \frac{t_a\times r_{ae}+t_b\times r_{be}+t_d\times r_{de}}{t_a+t_b+t_d} \\ &= \frac{0.6\times 0.9+0.2\times 0.5+0.2\times 0.1}{0.6+0.2+0.2} \\ &= 0.66 \\ R_{g\to t_{S\_DM_2}} &= \frac{t_a\times r_{ag}+t_b\times r_{bg}+t_d\times r_{dg}}{t_a+t_b+t_d} \\ &= \frac{0.6\times 0.2+0.2\times 0.4+0.2\times 0.7}{0.6+0.2+0.2} \\ &= 0.34 \\ R_{h\to t_{S\_DM_2}} &= \frac{t_a\times r_{ah}+t_b\times r_{bh}+t_d\times r_{dh}}{t_a+t_b+t_d} \\ &= \frac{0.6\times 0.3+0.2\times 0.5+0.2\times 0.6}{0.6+0.2+0.2} \\ &= 0.40 \end{aligned}$$

According to different contributions of the trust seniority, trust experience and trust recommendation to the trust degree, while taking the value $w_p = 0.2$, $w_e = 0.7$, $w_r = 0.1$ and $w_p + w_e + w_r = 1$, the trust degrees of e, g, and h for $t_{S\_DM_2}$ are comprehensively calculated as follows:

$$\begin{aligned} T_{e\to t_{S\_DM_2}} &= w_p\times P_{e\to t_{S\_DM_2}} + w_e\times E_{e\to t_{S\_DM_2}} \\ &\quad + w_r\times R_{e\to t_{S\_DM_2}} \\ &= 0.2\times 0.3+0.7\times 0.8+0.1\times 0.66 \\ &= 0.686 \\ T_{g\to t_{S\_DM_2}} &= w_p\times P_{g\to t_{S\_DM_2}} + w_e\times E_{g\to t_{S\_DM_2}} \\ &\quad + w_r\times R_{g\to t_{S\_DM_2}} \\ &= 0.2\times 0.55+0.7\times 0.56+0.1\times 0.34 \\ &= 0.536 \\ T_{h\to t_{S\_DM_2}} &= w_p\times P_{h\to t_{S\_DM_2}} + w_e\times E_{h\to t_{S\_DM_2}} \\ &\quad + w_r\times R_{h\to t_{S\_DM_2}} \\ &= 0.2\times 0.55+0.7\times 0.44+0.1\times 0.4 \\ &= 0.458 \end{aligned}$$

For the given threshold $H_{t_{S\_DM_2}} = 0.5$, it can be concluded that, $T_{e\to t_{S\_DM_2}} > T_{g\to t_{S\_DM_2}} > H_{t_{S\_DM_2}} > T_{h\to t_{S\_DM_2}}$, which indicates that e and g are more trustworthy than h.

5.2 Performance Evaluations for Security of the RDA_TC&CSS

5.2.1 Performance Evaluations Using the Simulated System

According to the result of the above analysis, e and g are considered as the trustworthy delegated objects. If γ_1 and γ_2 respectively represent the system status after implementing delegation on candidates e, and g, then for different collaborative strategy $cdod < \{DM, S\_DM_1, S\_DM_2, S\_DM_3, A\_DM\}, k >$, where $1 < k \leq 5$, Table 5 shows the minimal constraint set constructed by Algorithm 1, as well as descriptions for the satisfiability and security of γ_1 and γ_2. From the table, the following observations are presented.

1) C_1 can implicitly enforce e_1. Notice that $|\{Roles_{\gamma_1}(e) = \{A\_DM, S\_DM_2\}\} \cap \{DM, S\_DM_1, S\_DM_2, S\_DM_3, A\_DM\}| = 2 < 5$ and $|\{Roles_{\gamma_2}(g) = \{QP, S\_DM_2\}\}b \cap \{DM, S\_DM_1, S\_DM_2, S\_DM_3, A\_DM\}| = 1 < 5$, which indicates that γ_1 and γ_2 are satisfied to C_1 and are also secure to e_1. Thus, the more trusted assistant manager e should be selected for the delegation authorization in such case.

2) C_2, C_3, and C_4 can implicitly enforce e_2, e_3, and e_4, respectively, while notice that $|\{Roles_{\gamma_1}(e) = \{A\_DM, S\_DM_2\}\} \cap \{S\_DM_2, S\_DM_3, A\_DM\}| = 2$, which indicates that e violates $smer < \{S\_DM_2, S\_DM_3, A\_DM\}, 2 >$ in C_2, $smer < \{DM, S\_DM_2, S\_DM_3, A\_DM\}, 2 >$ in C_3, and $smer < \{DM, S\_DM_1, S\_DM_2, S\_DM_3, A\_DM\}, 2 >$ in C_4. γ_1 is unsatisfied to C_2, C_3 and C_4 and is also unsecure to e_2, e_3 and e_4. However, $Roles_{\gamma_2}(g) = \{QP, S\_DM_2\}$, which

Table 3: Completion effects

Measurement unit (k)	Empirical coefficient (w_{tk})	Completion effect (e_{ek})	Completion effect (e_{gk})	Completion effect (e_{hk})
1	0.2	-	-	0.7
2	0.4	-	0.6	-
3	0.6	-	-	0.5
4	0.8	-	0.4	-
5	1.0	0.8	-	-

Table 4: Trust recommendations

Referee (u_{rk})	Trust value of referee (t_k)	Recommendation value (r_{ke})	Recommendation value (r_{kg})	Recommendation value (r_{kh})
a	0.6	0.9	0.2	0.3
b	0.2	0.5	0.4	0.5
d	0.2	0.1	0.7	0.6

indicates that g meets any constraint requirement from C_2, C_3 and C_4, and then γ_2 is also secure to e_2, e_3 and e_4. Thus, only the inspector g is selected as the delegated object in such cases, in order to ensure the security of the system status.

5.2.2 Performance Evaluations Using the Real-world Datasets

To further evaluate the efficiency of the algorithm for the construction of SMER constraints, we consider the real-world datasets used in the work [14]. However, the Domino, Firewall1, Firewall2, and Healthcare datasets could not reflect the performance of the proposal, since some users in these datasets violate the security strategies, from which valid SMERs cannot be generated. Thus, only five datasets are taken into consideration for the experiments, including Americas-large, Americas-small, Apj, Customer, and Emea. Further, the regular mining tool RMiner [11] is used for mining the initial roles with no constraints, as well as UA.

Different types of the $k-n$ CDOD strategy are synthetically generated using a simulator. In terms of the length of constraint enforcement, we study four different cases: 2-2 CDOD, 2-3 CDOD, 3-5 CDOD, and 5-10 CDOD, where n permissions are randomly chosen from the set of all permissions. Meanwhile, the sizes of $k-n$ CDOD are fixed as 30, and 50, respectively. We consider the initial mining results and the $k-n$ CDOD constraints as inputs and repeatedly conduct the experiments 20 times. The average time for constructing SMERs from different CDOD strategies, as well as the results of the compared methods RMP_SoD and RMO_SODSDA, are shown in Tables 6 $\sim$ 13, where Ek-n CDOD indicates the CDOD strategy, and $C_{t-mSMER}$ indicates the SMER constraint set.

When $|E_{k-nCDOD}| = 30$, it is intuitively observed from Tables 6 $\sim$ 9 that, the time needed for construction of the t-t SMERs grows rapidly as the length of the CDOD strategy increases. Take the Americas-large dataset as an example, and the length of CDOD changes from 2 to 10. The time for constructing t-t SMERs is 149, 511, 2078, and 6267s, respectively. Similarly, the time needed for construction of the $t-m$ SMERs is 289, 567, 1315, and 7771s, respectively, which also grows rapidly as the length of the CDOD strategy increases. However, most of the time taken for the latter is longer than that of the former. This is because the t-t SMER is more restricted than the $t-m$ SMER, and the number of constructing $t-m$ SMERs should be greater than that of constructing t-t SMERs. Thus, the time cost for the construction is longer with the increasing number of constraints. Similar to the above analysis for $|E_{k-nCDOD}| = 30$, the detailed analysis of the time taken for $|E_{k-nCDOD}| = 50$, as shown in Tables 10 $\sim$ 13, is omitted owing to the limited space.

A further observation from Tables 6 $\sim$ 13 is that, the time taken for construction of SMERs using different methods are comparable. Specifically, taking the Americas-small dataset as an example, when $|E_{2\text{-}3CDOD}| = 30$, the time taken for construction of $C_{t-mSMER}$ using the three methods is 28, 29, and 28s, respectively; when $|E_{3\text{-}5CDOD}| = 30$, the time for $C_{t-mSMER}$ using these methods is 91, 92, and 94, respectively. Thus, RDA_TC&CSS performs as well as the RMP_SoD and RMO_SODSDA methods, in order to ensure the system security, while improving the reliability of the delegation process.

Table 5: Enforcement of the Security Strategy

$k-n$ CDOD	$t-m$ SMER	$sat(\gamma_1)$	$sec(\gamma_1)$	$sat(\gamma_2)$	$sec(\gamma_2)$
$e_1 = cdod < \{DM, S\_DM_1, S\_DM_2, S\_DM_3, A\_DM\}, 2 >$	$C_1 = \{smer < \{DM, S\_DM_1, S\_DM_2, S\_DM_3, A\_DM\}, 5 >\}$	$sat_{C_1}(\gamma_1) = 1$	$sec_{e_1}(\gamma_1) = 1$	$sat_{C_1}(\gamma_2) = 1$	$sec_{e_1}(\gamma_2) = 1$
$e_2 = cdod < \{DM, S\_DM_1, S\_DM_2, S\_DM_3, A\_DM\}, 3 >$	$C_2 = \{smer < \{DM, S\_DM_1, S\_DM_2\}, 2 >, smer < \{DM, S\_DM_1, S\_DM_3\}, 2 >, smer < \{DM, S\_DM_1, A\_DM\}, 2 >, smer < \{DM, S\_DM_2, S\_DM_3\}, 2 >, smer < \{DM, S\_DM_2, A\_DM\}, 2 >, smer < \{DM, S\_DM_3, A\_DM\}, 2 >, smer < \{S\_DM_1, S\_DM_2, S\_DM_3\}, 2 >, smer < \{S\_DM_1, S\_DM_2, A\_DM\}, 2 >, smer < \{S\_DM_1, S\_DM_3, A\_DM\}, 2 >, smer < \{S\_DM_2, S\_DM_3, A\_DM\}, 2 >, smer < \{DM, S\_DM_1, S\_DM_2, S\_DM_3, A\_DM\}, 3 >\}$	$sat_{C_2}(\gamma_1) = 0$	$se_{e_2}(\gamma_1) = 0$	$sat_{C_2}(\gamma_2) = 1$	$se_{e_2}(\gamma_2) = 1$
$e_3 = cdod < \{DM, S\_DM_1, S\_DM_2, S\_DM_3, A\_DM\}, 4 >$	$C_3 = \{smer < \{DM, S\_DM_1, S\_DM_2, S\_DM_3\}, 2 >, smer < \{DM, S\_DM_1, S\_DM_2, A\_DM\}, 2 >, smer < \{DM, S\_DM_1, S\_DM_3, A\_DM\}, 2 >, smer < \{DM, S\_DM_2, S\_DM_3, A\_DM\}, 2 >, smer < \{S\_DM_1, S\_DM_2, S\_DM_3, A\_DM\}, 2 >\}$	$sat_{C_3}(\gamma_1) = 0$	$sec_{e_3}(\gamma_1) = 0$	$sat_{C_3}(\gamma_2) = 1$	$sec_{e_3}(\gamma_2) = 1$
$e_4 = cdod < \{DM, S\_DM_1, S\_DM_2, S\_DM_3, A\_DM\}, 5 >$	$C_4 = \{smer < \{DM, S\_DM_1, S\_DM_2, S\_DM_3, A\_DM\}, 2 >\}$	$sat_{C_4}(\gamma_1) = 0$	$sec_{e_4}(\gamma_1) = 0$	$sat_{C_4}(\gamma_2) = 1$	$sec_{e_4}(\gamma_2) = 1$

Table 6: Performance comparison when $|E_{2\text{-}2CDOD}| = 30$

Dataset	**RMP_SoD(s)**		**RMO_SODSDA(s)**		**RDA_TC&CSS(s)**	
	$C_{t-tSMER}$	$C_{t-mSMER}$	$C_{t-tSMER}$	$C_{t-mSMER}$	$C_{t-tSMER}$	$C_{t-mSMER}$
Americas-large	139.7	279.5	144.7	281.5	149.5	289.5
Americas-small	10.1	17.2	10.1	18.1	13.1	20.2
Apj	0.4	0.8	0.4	0.8	0.4	0.9
Customer	0.3	0.4	0.3	0.4	0.3	0.4
Emea	0.01	0.04	0.02	0.04	0.02	0.06

Table 7: Performance comparison when $|E_{2\text{-}3CDOD}| = 30$

Dataset	**RMP_SoD(s)**		**RMO_SODSDA(s)**		**RDA_TC&CSS(s)**	
	$C_{t-tSMER}$	$C_{t-mSMER}$	$C_{t-tSMER}$	$C_{t-mSMER}$	$C_{t-tSMER}$	$C_{t-mSMER}$
Americas-large	505.5	552.9	509.5	552.9	511.7	567.3
Americas-small	30.5	28.3	31.8	29.3	32.2	28.7
Apj	1.4	1.2	1.4	1.2	1.4	1.5
Customer	0.3	0.3	0.3	0.3	0.3	0.3
Emea	0.07	0.06	0.07	0.06	0.07	0.06

Table 8: Performance comparison when $|E_{3\text{–}5CDOD}| = 30$

Dataset	RMP_SoD(s)		RMO_SODSDA(s)		RDA_TC&CSS(s)	
	$C_{t-tSMER}$	$C_{t-mSMER}$	$C_{t-tSMER}$	$C_{t-mSMER}$	$C_{t-tSMER}$	$C_{t-mSMER}$
Americas-large	2022.7	1314.7	2054.3	1314.7	2078.4	1315.9
Americas-small	117.5	91.9	133.6	92.9	144.1	94.8
Apj	6.7	4.5	7.1	4.6	8.7	4.5
Customer	1.2	3.2	5.0	3.5	5.6	3.2
Emea	0.3	0.2	0.3	0.2	0.3	0.2

Table 9: Performance comparison when $|E_{5\text{–}10CDOD}| = 30$

Dataset	RMP_SoD(s)		RMO_SODSDA(s)		RDA_TC&CSS(s)	
	$C_{t-tSMER}$	$C_{t-mSMER}$	$C_{t-tSMER}$	$C_{t-mSMER}$	$C_{t-tSMER}$	$C_{t-mSMER}$
Americas-large	6164.6	7771.9	6267.3	7778.4	6267.3	7771.9
Americas-small	260.7	460.5	371.4	465.7	371.4	464.5
Apj	19.7	28.9	23.3	29.9	23.3	29.3
Customer	0.9	34.8	28.1	36.8	28.1	35.7
Emea	0.7	0.8	0.7	0.8	0.7	0.8

Table 10: Performance comparison when $|E_{2\text{–}2CDOD}| = 50$

Dataset	RMP_SoD(s)		RMO_SODSDA(s)		RDA_TC&CSS(s)	
	$C_{t-tSMER}$	$C_{t-mSMER}$	$C_{t-tSMER}$	$C_{t-mSMER}$	$C_{t-tSMER}$	$C_{t-mSMER}$
Americas-large	366.2	759.1	379.5	759.1	386.1	759.1
Americas-small	29.2	60.4	30.2	60.4	33.2	62.7
Apj	0.9	2.4	1.2	2.4	1.4	2.6
Customer	0.01	1.1	0.5	1.1	0.5	1.1
Emea	0.05	0.12	0.06	0.12	0.06	0.12

Table 11: Performance comparison when $|E_{2\text{–}3CDOD}| = 50$

Dataset	RMP_SoD(s)		RMO_SODSDA(s)		RDA_TC&CSS(s)	
	$C_{t-tSMER}$	$C_{t-mSMER}$	$C_{t-tSMER}$	$C_{t-mSMER}$	$C_{t-tSMER}$	$C_{t-mSMER}$
Americas-large	1203.9	1078.1	1212.8	1078.1	1211.9	1070.7
Americas-small	89.9	85.6	96.3	85.6	97.4	85.6
Apj	3.6	2.7	3.1	2.7	3.0	2.3
Customer	1.3	0.6	0.7	0.6	0.6	0.5
Emea	0.02	0.1	0.1	0.1	0.1	0.1

Table 12: Performance comparison when $|E_{3\text{–}5CDOD}| = 50$

Dataset	RMP_SoD(s)		RMO_SODSDA(s)		RDA_TC&CSS(s)	
	$C_{t-tSMER}$	$C_{t-mSMER}$	$C_{t-tSMER}$	$C_{t-mSMER}$	$C_{t-tSMER}$	$C_{t-mSMER}$
Americas-large	5762.9	3751.6	5861.9	3753.1	5872.2	3751.6
Americas-small	280.9	216.2	337.9	223.4	341.9	216.2
Apj	17.9	12.6	19.7	14.5	22.6	12.6
Customer	2.7	7.7	12.1	8.8	15.5	7.7
Emea	0.8	0.5	0.8	0.7	0.8	0.6

Table 13: Performance comparison when $|E_{5\text{–}10CDOD}| = 50$

Dataset	RMP_SoD(s)		RMO_SODSDA(s)		RDA_TC&CSS(s)	
	$C_{t-tSMER}$	$C_{t-mSMER}$	$C_{t-tSMER}$	$C_{t-mSMER}$	$C_{t-tSMER}$	$C_{t-mSMER}$
Americas-large	14667.3	18612.1	15008.8	18876.6	15001.9	18612.1
Americas-small	5.9	1116.7	900.5	1155.1	897.1	1116.7
Apj	47.0	73.6	59.4	87.7	66.0	73.6
Customer	2.3	87.4	70.5	86.1	74.3	87.4
Emea	1.7	0.8	0.7	0.7	0.8	0.8

5.3 Discussion

From the above analysis for the reliability and security of the delegation-authorization process, we find the main benefits of the RDA_TC&CSS as follows.

1) Most of the existing delegation approaches have the problem of arbitrariness. The delegation process is unreliable and untrustworthy, and there exists the danger of abuse of privileges once the delegated object h with lower trustworthiness is selected. To improve the reliability of the delegation process, the proposed method comprehensively computes the trust degrees of different candidate objects based on quantitative analysis for the trust seniority, trust experience and trust recommendation. It eliminates the object h with low trust degree from the candidate set, and then chooses e, g as the trustworthy objects. Thus, the delegated object chosen via the RDA_TC&CSS becomes much more reliable.

2) On the basis of ensuring the reliability of the delegation process, the collaborative division strategies e_2, e_3, and e_4 in the simulated system are violated using the existing delegation approaches, and the security of the system status will be compromised after delegation. To ensure the system security, the proposed method utilizes the method of constructing the minimal set of mutually-exclusive-role constraints, which indirectly implements the collaborative security strategy, in order to further determine the most appropriate delegated object g in the specific collaborative scenario, while satisfying various constraint requirements of systems.

3) The proposed algorithm in the article intuitively reflects the satisfaction requirements of the system status. The time complexity for construction of the $t-m$ SMERs depends on the double loops. The execution number of the outer loop is $(\lfloor \frac{n-1}{k-1} \rfloor - 2)$; in the inner loop, for the particular m, it is necessary to combine any m roles from n roles in the collaboration. Thus, the total time complexity of the algorithm is $O(2^n)$. The efficiency of the algorithm decreases obviously as the value of n increases. In general, if m is small, then the efficiency of the algorithm is acceptable.

Compared to the existing research approaches, features of the proposal are presented as shown in Table 14, where a tick V indicates that the feature is available.

Nevertheless, the RDA_TC&CSS still has the limitation: As shown in Table 5, for the given collaborative division strategies e_1, e_2, e_3 and e_4 as well as the minimal constraint sets C_1, C_2, C_3 and C_4, it is seen that e_1, e_4 can be precisely enforced by C_1, and C_4, respectively. However, e_2, e_3 cannot be enforced by C_2 or C_3. Therefore, the minimal constraint set constructed by the algorithm may not be able to precisely implement the CDOD strategy.

6 Conclusions

A novel delegation-authorization method based on RBAC, called RDA_TC&CSS, was proposed in this study. First, we utilized the trust seniority, trust experience and trust recommendation to comprehensively compute the trust degrees of different candidate objects, and then chose the objects with higher values. Next, we adopted the collaborative security strategy to further determine the most appropriate delegated object in the specific collaborative scenario. Further, we presented the algorithm to indirectly implement the collaborative strategy by constructing the minimal set of constraints and verified the correctness of the algorithm. The experiments using a specific simulated system and the real-world datasets demonstrated that, the proposed method could improve the reliability of the delegation process, while ensuring the system security. Our future work will focus on studying how to implement the RDA_TC&CSS in practical scenarios such as the IoT, blockchain, and wireless sensor networks.

References

[1] D. Abdelfattah, H. A. Hassan, and F. A. Omara, "Enhancing highly-collaborative access control system using a new role-mapping algorithm," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 3, p. 2765, 2022.

[2] A. M. Abdul, A. A. K. Mohammad, P. Venkat Reddy, P. Nuthakki, R. Kancharla, R. Joshi, and N. Kan-

Table 14: Comparison of features

Feature	Sun *et al.* [21]	Pal *et al.* [16]	Ali *et al.* [4]	Khan *et al.* [9]	Abdul *et al.* [2]	Proposed method
Detailed implementation of delegation process	-	-	-	-	-	V
Fine-grained delegation	-	-	V	-	-	V
Reliability analysis	-	-	-	V	V	V
Security analysis	V	V	V	V	V	V

naiya Raja, "Enhancing security of mobile cloud computing by trust-and role-based access control," *Scientific Programming*, vol. 2022, pp. 1–10, 2022.

[3] M. U. Aftab, Z. Qin, N. W. Hundera, O. Ariyo, N. T. Son, and T. V Dinh, "Permission-based separation of duty in dynamic role-based access control model," *Sycmmetry*, vol. 11, no. 5, p. 669, 2019.

[4] G. Ali, N. Ahmad, Y. Cao, M. Asif, H. Cruickshank, and Q. E. Ali, "Blockchain based permission delegation and access control in Internet of Things (BACI)," *Computers & Security*, vol. 86, pp. 318–334, 2019.

[5] F. A. Alsulaiman, A. Miege, and A. E. Saddik, "Threshold-based collaborative access control(T-CAC)," in *Proceedings of International Symposium on Collaborative Technologies and Systems*, pp. 46–56, 2007.

[6] S. Ameer, J. Benson, and R. Sandhu, "Hybrid approaches (ABAC and RBAC) toward secure access control in smart home IoT," *IEEE Transactions on Dependable and Secure Computing*, 2022. doi: 10.1109/TDSC.2022.3216297.

[7] J. Crampton and H. Khambhammettu, "Delegation in role-based access control," *International Journal of Information Security*, vol. 7, no. 2, pp. 123–136, 2008.

[8] M. Ghafoorian, D. Abbasinezhad-Mood, and H. Shakeri, "A thorough trust and reputation based RBAC model for secure data storage in the cloud," *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 4, pp. 778–788, 2019.

[9] K. H. Khan, I. U. Din, A. Almogren, H. A. Khattak, M. Ibrahim, and S. Nazir, "Secure delegation using enhanced capability model," *Security and Communication Networks*, vol. 2022, pp. 1–9, 2022.

[10] B. Lang, J. Wang, and Y. Liu, "Achieving flexible and self-contained data protection in cloud computing," *IEEE Access*, vol. 2017, no. 5, pp. 1510–1523, 2017.

[11] R. Li, H. Li, W. Wei, X. Ma, and X. Gu, "RMiner: a tool set for role mining," in *Proceedings of the 18th ACM Symposium on Access Control Models and Technologies*, pp. 193–196, 2013.

[12] F. Liu and C. Chang, "Access control model based on multidimensional measurement and context," *Computer Engineering*, vol. 37, no. 24, pp. 129–131, 135, 2011.

[13] W. Liu, H. Duan, H. Zhang, P. Ren, and J. Wu, "TRBAC: trust-based access control model," *Journal of Computer Research and Development*, vol. 48, no. 8, pp. 1414–1420, 2011.

[14] B. Mitra, S. Sural, J. Vaidya, and V. Atluri, "A Survey of Role Mining," *ACM Computing Surveys*, vol. 48, no. 4, pp. 1–37, 2016.

[15] F. Nazerian, H. Motameni, H. Nematzadeh, "Emergency role-based access control (E-RBAC) and analysis of model specifications with alloy," *Journal of Information Security and Applications*, vol. 45, pp. 131–142, 2019.

[16] S. Pal, T. Rabehaja, M. Hitchens, V. Varadharajan, and A. Hill, "On the design of a flexible delegation model for the Internet of Things using blockchain," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3521–3530, 2020.

[17] A. Roy, S. Sural, A. K. Majumdar, J. Vaidya, and V. Atluri, "Enabling workforce optimization in constrained attribute-based access control systems," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 4, pp. 1901–1913, 2019.

[18] P. Sarana, A. Roy, S. Sural, J. Vaidya, and V. Atluri, "Role mining in the presence of separation of duty constraints," in *Proceedings of the 11th International Conference (ICISS'15)*, pp. 98-117, 2015.

[19] W. Sun, H. Su, and H. Xie, "Policy-engineering optimization with visual representation and separation-of-duty constraints in attribute-based access control," *Future Internet*, vol. 12, no. 10, p. 164, 2020.

[20] W. Sun, S. Wei, H. Guo, and H. Liu, "Role-mining optimization with separation-of-duty constraints and security detections for authorizations," *Future Internet*, vol. 11, no. 9, p. 201, 2019.

[21] W. Sun, X. Yuan, and H. Su, "Role-engineering optimization with user-oriented cardinality constraints in role-based access control," *International Journal of Network Security*, vol. 23, no. 5, pp. 845–855, 2021.

[22] C. Uikey and D. S. Bhilare, "RBACA: Role-based access control architecture for multi-domain cloud environment," *International Journal of Business Information Systems*, vol. 28, no. 1, pp. 1–17, 2018.
[23] G. Yu, R. Li, Z. Lu, W. Song, and Z. Tang, "Locale-based access control model in collaborative environment," *Computer Science*, vol. 36, no. 1, pp. 81–85, 2009.
[24] J. Zhang, T. Li, Z. Ying, and J. Ma, "Trust-based secure multi-cloud collaboration framework in cloud-fog-assisted IoT," *IEEE Transactions on Cloud Computing*, 2022.
[25] Y. Zhu, "Dynamic multi-level access control model based on user trust," *Computer Engineering*, vol. 37, no. 23, pp. 129–131, 2011.

Biography

Wei Sun received his B.S. and M.S. degrees from the School of Information Engineering, Zhengzhou University, China, in 2003 and 2008, respectively. He is currently working in the School of Computer and Information Technology, Xinyang Normal University. His current research interests include access control and system security.

Privacy Protection Data Aggregation Scheme Based on Horner Rule and Lightweight Convolutional Neural for Intelligent Education

Jian Zhang

(Corresponding author: Jian Zhang)

Zhengzhou Medical College

No.3 Chuangye Avenue, Chaohua New District, Xinmi City, Zhengzhou 452385

Email: zzll_201@foxmail.com

(Received Jan. 15, 2023; Revised and Accepted June 16, 2023; First Online June 25, 2023)

The Special Issue on Computational Intelligence Networks for Privacy and Security in Evolving Internet of Multimedia Things

Special Editor: Prof. Shoulin Yin (Harbin Institute of Technology)

Abstract

In the context of digitized education, campuses have been the worst hit areas of cyber attacks, ransomware, and information leakage. Therefore, we propose a novel privacy protection data aggregation scheme based on the Horner rule and lightweight convolutional neural for intelligent education. This scheme uses the Horner rule to aggregate multi-user and multi-regional educational data in a multi-dimensional way. A lightweight convolutional neural network is used to extract data features, and homomorphic encryption is used to ensure user data privacy. Fine-grained access control of aggregated data is achieved using proxy re-encryption; only a specified authorized entity can read the aggregated data. The security analysis shows that the proposed scheme can ensure user privacy and data integrity and carry out fine-grained access control on aggregated data, which can better meet the needs of practical applications.

Keywords: Data Aggregation; Horner Rule; Intelligent Education; Lightweight Convolutional Neural; Privacy Protection

1 Introduction

With the development of science and technology, people's life has become more information and intelligent, and the education system has gradually changed to intelligent education. Intelligent education collects students' behavioral data through different sensors, and then uploads the behavioral data to the control center, which dynamically allocates educational resources through statistical analysis of a large number of data. At the same time, intelligent education can also provide customized learning methods for user groups with different educational needs in different regions based on the analysis results [9,10]. Compared with traditional power grid, intelligent education can provide richer functions, better performance and higher reliability. Although intelligent education has made great progress in recent years, it still faces security threats in three aspects.

1) Privacy of user education data. The data in different time periods potentially reflect users' personal privacy. For example, relatively low behavioral data in a time period may mean less student behavior in that time period. When malicious attackers get these data, they will violate users' personal privacy and even provide information for some real crimes.

2) Integrity of user data. If the user data is tampered or forged by malicious attackers in the transmission process, it will not only affect the correct evaluation of students' behavior, but also affect the normal allocation of teaching resources.

3) Control of access to aggregated data. Most of the existing data aggregation schemes can only read the aggregated data in a single control center, without considering the presence of multiple data receivers. For example, switch between the active and standby control centers or switch between different administrators in the same control center. Different data receivers should also have limited access to aggregated data. For example, the administrator of a region can read only the aggregated data of the region, and the administrator with higher permission can read the aggregated data of all regions.

To solve the above problems, this paper proposes a privacy protection data aggregation scheme that supports fine-grained access control in intelligent education.

Firstly, this paper considers multi-dimensional data aggregation. In addition to the aggregation of different users' data in any region, it also considers the aggregation of students' data in different regions, and uses Horner's rule to compress the aggregated data of different dimensions to ensure that the data of each dimension can still be recovered after aggregation. In addition, this paper uses a lightweight neural network to extract data features, and encrypts each user's educational data with homomorphic encryption technology, so as to ensure the privacy of user data, and also requires that the data can be operated in the encrypted state. To ensure the integrity of encrypted data during storage and transmission, digital signatures are used to verify data integrity, and batch authentication is used to improve the efficiency of authentication. Finally, the proxy re-encryption technology is used to re-encrypt the aggregated data with the public key of the specified receiver to ensure that only the specified receiver can decrypt the aggregated data and achieve fine-grained access control.

This paper is divided into eight parts. Section 2 shows the related works including homomorphic encryption and horner rule. Section 3 introduces system model and security requirements. Section 4 proposes the new data aggregation scheme. Section 5 shows the security analysis. Security attribute comparison is stated in Section 6. Section 7 shows the efficiency analysis. There is a conclusion in Section 8.

2 Related Works

2.1 Homomorphic Encryption

Suppose there are K plaintext $m_i (i = 1, 2, \cdots, K)$, Enc_{pk} means encryption using the public key pk, Dec_{sk} means decryption using the corresponding private key sk. The addition homomorphic property can be expressed as:

$$Dec_{sk}(\prod_{i=1}^{K} Enc_{pk}(m_i)) = \sum_{i=1} m_i. \quad (1)$$

Paillier encryption [21] is the most typical public-key encryption algorithm with homomorphic property of addition. Specifically, it consists of the following four algorithms.

1) Initialization. Select the safety parameter κ. p_1 and q_1 are two large prime numbers, and it satisfies $L(p_1) = L(q_1) = \kappa$, calculates $N = p_1 q_1$ and $\lambda = lcm(p_1 - 1, q_1 - 1)$, where lcm represents the solution of the least common multiple. Define $L(u) = (U - 1)/N$, $g = N + 1$, and calculate $\mu = (L(g^{\lambda} mod N^2))^{-1}$.

2) Key generation. The public key is $pk = (N, g)$, and the private key is $sk = (\lambda, \mu)$.

3) Encryption. Assuming that the message to be encrypted is $M \in Z_N$, select a random number $r \in Z_N^*$, and calculate the ciphertext $C = Enc_{pk}(M) = g^M r^N mod N^2$.

4) Decryption. Assuming that the ciphertext to be decrypted is $C \in Z_{N^2}^*$, the plaintext message $M = Dec_{sk}(C) = L(C^{\lambda} mod N^2)\mu mod N$ can be recovered using the private key.

2.2 Horner Rule

Horner rule is an efficient algorithm to evaluate polynomials [2,12], which can transform the evaluation problem of n degree polynomials into the evaluation of n degree polynomials and simplify the calculation process. For example, $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ can be converted to $p(x) = (\cdots (a_n x + a_{n-1})x + \cdots)x + a_0$. And more specifically, by limiting $x > max a_n, a_{n-1}, \cdots, a_1$, it can recover n coefficients $a_1, a_2, \cdots, a_n$ of a polynomial by n-division and n-modular operation, given x and $p(x)$.

3 System Model and Security Requirements

3.1 System Model

The symbols used in this article and their corresponding meanings are shown in Table 1. The system model is shown in Figure 1. The system proposed in this paper consists of five entities, namely, user-oriented intelligent classroom (User), region-oriented area aggregation gateway (RAGW), data center (DC), access control center (ACC), and data receiver (DR).

Table 1: Symbols and their corresponding meanings

Symbol	Name
$RAGW_1$	Area aggregation gateway of area i
$User_{ik}$	The $k-th$ smart classroom in area i
$BAMDD_i$	Multidimensional aggregated ciphertext data in area i
SAMDD	All multidimensional aggregated ciphertext data
N, g, G	EDD Encryption parameter
H	Hash function
R_1, R_2	Horner parameter
m	Total area number
n	Maximum number of users in each area
n_i	Number of actual users in area i
D	The maximum value of data in a single dimension
C_{ik}	Encrypted ciphertext of d_{ik}

1) Smart classroom. This entity is the terminal device of intelligent education, responsible for collecting user data, and using encryption and digital signature

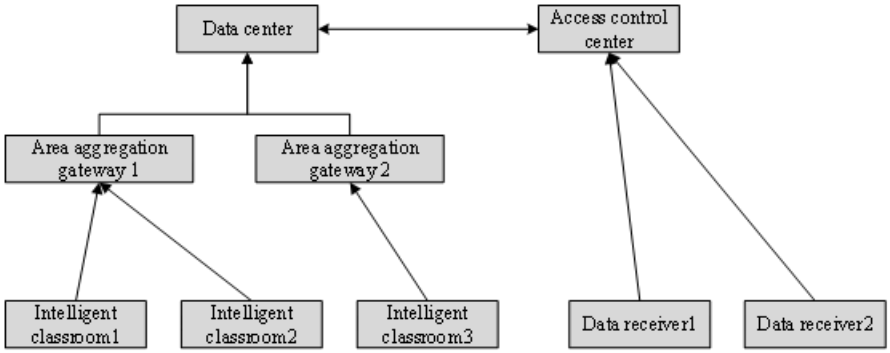


Figure 1: The proposed scheme

respectively to ensure the privacy and integrity of the data, and finally send the encrypted data to the area aggregation gateway [6].

2) Area aggregation gateway. The entity is responsible for managing smart classrooms in an area. After receiving ciphertext data from n smart classrooms in an area, the entity first verifies the integrity of the data, aggregates the student data in the area, and finally sends the aggregation result to the data center [8].

3) Data center. This entity is responsible for re-aggregating student data across regions. When an authorized data receiver initiates an access request to the aggregated data, the proxy reencryption scheme is invoked and the public key of the recipient is used to re-encrypt the ciphertext. The data center performs some proxy re-encryption operations.

4) Access control center. The entity is responsible for authenticating multiple data receivers and managing access rights, and performing another part of the agent re-encryption operation. The combination of the two parts of the operation can realize the complete agent re-encryption function.

5) Data receiver. This entity is responsible for reading aggregate data, analyzing and applying it accordingly.

3.2 Adversary Model and Security Requirements

In this scenario, it is assumed that all entities are honest and curious, that they will perform various operations in accordance with the agreement, but may try to obtain private information outside of their authority [14, 19]. Also, assume that the data center and the access control center are not conspiring. Typically, you can outsource the data center to one cloud computing platform and the access control center to another competing cloud computing platform. An external adversary A may attempt to obtain the user's electricity usage information, tamper with the electricity usage data or obtain aggregated data outside the authority, assuming that the adversary has the following capabilities.

- A can eavesdrop on all transmission channels and obtain transmitted ciphertext information.
- A can control the access control center or the data center, but not both at the same time. Once the access control center or data center is controlled by A, A will have access to all its internal state information.

A privacy protection data aggregation scheme in intelligent education needs to meet the following security requirements.

1) Correctness. The solution itself needs to be correct, that is, the protocol involved can be executed correctly.

2) Privacy. Even if an adversary has these capabilities, individual user data information cannot be accessed, and aggregated student data cannot be accessed by unauthorized data recipients.

3) Integrity. After an adversary modifies or forges data, the system can detect the malicious operation in time. The aggregation operation can be performed by the area aggregation gateway and data center only after data integrity verification.

4) Fine-grained access control. Only authorized data receivers can read the corresponding aggregated data, and authorized data receivers cannot obtain data outside of their permissions.

4 Proposed Data Aggregation Scheme

The scheme proposed in this paper includes seven stages: system initialization, data feature extraction, user data reporting, regional data aggregation, total data aggregation, data request, and data processing.

4.1 System Initialization

1) Select security parameter κ and call $Gen(\kappa)$ to generate bilinear pairing parameters (q, P, G_1, G_2, e). Select the security parameter κ_1 and call the key generation algorithm of the HERS scheme to get the parameters of EDD encryption $(N = p_1q_1, g, G)$. Finally, select a hash function $H : 0, 1^* \rightarrow G_1$.

2) The access control center sends registration requests to the data center.

3) The public and private key pairs generated by the data center are $sk_{DC} = a, pk_{DC} = g^a$.

4) The access control center generates the public and private key pairs $sk_{ACC} = b, pk_{ACC} = g^b$.

5) The $PK = pk_{DC}^{sk_{ACC}} = pk_{ACC}^{sk_{DC}} = g^{a \cdot b} mod N^2$ is obtained after the key negotiation between the data center and the access control center.

6) Data center select two Horner parameters as $R_1 > nD$, $R_2 > nD$.

7) The data center exposes parameter is $(q, P, G_1, G_2, e, N, g, G, H, R_{1,2}$.

4.2 Feature Extraction

In this paper, the basic architecture of PeleeNet is followed [16, 18], and the above method is improved. The two-way dense layer and the conversion layer 1×1 standard convolution layer are replaced by 1×1 GSD-Channel-Wise, and GSDCPeleeNet is proposed. The output dimensions of each layer are consistent with PeleeNe. In ShuffleNet practical criteria for efficient network design, it is pointed out that large packet convolution will increase memory access cost and lead to lower model speed. Considering the influence of precision and speed, the number of groups is set as 2 in 1×1 GSD-Channel-Wise convolution. In this convolutional layer, the step size s in the direction of the long volume kernel channel is selected as the hyperparameter, which can be adjusted according to the required precision and number of parameters. Four models, GSDCPeleeNe-sl, GSDCPeleeNe-s32, GSDCPeleeNe-s64 and GSDCPeleeNe-s192, are designed in this paper, and their step sizes in the direction of the channel are 1, 32, 64 and 192, respectively. Their total parameters range from 1.11 M to 1.808 M, accounting for 39.6% to 64.5% of PeleeNet(2.8 M).

The complexity of a network model is often measured by floating-point Operations (FLOPS), which can be interpreted as computational work. For the convolution layer, the computational quantity formula is:

$$FLOPS = (2mK^2 - 1) \times H \times W \times n. \tag{2}$$

Where, m is the number of channels in the input feature graph, K is the size of the convolution kernel, H and W are the size of the output feature graph, and n is the number of output channels. For the fully connected layer, the calculation quantity formula is:

$$FLOPS = (2I - 1) \times O. \tag{3}$$

Where I is the number of incoming neurons and O is the number of outgoing neurons. After calculation, the calculation amount of GSDCPeleeNet is 178.6 MFLOPs, which is 35.1% of PeleeNet(508 MFLOPs).

4.3 User Data Reporting

1) Intelligent education User collects multi-dimensional student information $(d_{ik1}, d_{ik2}, \cdots, d_{ikl})$, calculate $d_{iw} = R_2^i(R_1^1 d_{ikl} + R_1^2 d_{ik2} + \cdots + R_1^l d_{ikl})$, using PK to encrypt data as:

$$\begin{aligned} C_{ik} &= Enc_{PK}(d_{ik}) \\ &= PK^r(1 + d_{ik}N), g^r(modN^2) \end{aligned} \tag{4}$$

2) The intelligent education $User_{ik}$ signs the ciphertext, as shown in Formula (5).

$$\sigma_{ik} = x_{ik} H(C_{ik}||ID\_RAGW_i||ID\_User_{ik}||T). \tag{5}$$

3) The intelligent education $User_{ik}$ constructs D_{ik} and sends it to the area aggregation gateway $RAGW_i$, as shown in Formula (6).

$$D_{ik} = C_{ik}||ID_RAGW_i||ID\_User_{ik}||T||\sigma_{ik}. \tag{6}$$

4.4 Area Data Aggregation

1) Area aggregation gateway $RAGW_i$ will receive n_i user data reports D_{ik}. $Set_i = (D_{i1}, D_{i2}, \cdots, D_{i,n_i})$ is randomly divided into two sets $Set_{i1}(|Set_{i1}| = \frac{n_i}{2})$, $Set_{i2}(|Set_{i2}| = \frac{n_i}{2})$.

2) Batch validation, that is, verify Formula (7) and Formula (8).

$$\begin{aligned} e(P, \sum_{D_{ir} \in Set_{i1}} \sigma_{ir}) = \prod_{D_{ir} \in Set_{i1}} \\ e(Y_{ir}, H(C_{ir}||ID\_RAGW_i|| \\ ID\_User_{ir}||T)) \end{aligned} \tag{7}$$

$$\begin{aligned} e(P, \sum_{D_{ir} \in Set_{i2}} \sigma_{ir}) = \prod_{D_{ir} \in Set_{i2}} \\ e(Y_{ir}, H(C_{ir}||ID\_RAGW_i|| \\ ID\_User_{ir}||T)) \end{aligned} \tag{8}$$

3) After the batch verification is passed, it is necessary to establish some virtual data $C_{i,n_i+1}, C_{i,n_i+2}, C_{in}$, so that the number of user reports for each region is the same, as shown in Formula (9).

$$C_{ik} \quad = Enc_{PK}(d_{ik}). \tag{9}$$

4) The area aggregation gateway aggregates all ciphertexts, as shown in Formula (10).

$$BAMDD_i = \prod_{k=1}^{n} C_{ik}(modN^2). \tag{10}$$

5) The area aggregation gateway signs the aggregated ciphertext, as shown in Formula (11).

$$\sigma_i = x_i H(BAMDD_i||ID\_DGW_i||ID\_RAGW_i||n_i||T). \tag{11}$$

6) Area aggregation gateway $RAGW_i$ constructs D_i and sends it to the data center, as shown in Formula (12).

$$D_i = BAMDD_i||ID\_DGW||ID_RAGW_i||n_i||T||\sigma_i. \tag{12}$$

4.5 Aggregate Data Aggregation

- Data centers use a similar approach to regional data aggregation for $D_1, D_2, \cdots, D_m$ performing batch verification [4, 15].
- After the batch authentication is successful, the data center performs secondary aggregation for all ciphertexts. For different access policies, you can select only a few areas with the same permission level to aggregate ciphertext for secondary aggregation, as shown in Formula (13).

$$SAMDD = \prod_{i=1}^{m} BAMDD_i modN^2. \tag{13}$$

4.6 Data Request

1) Data receiver DR_j sends an access request for aggregated data to the access control Center.

2) After identifying the authorized data receiver, the access control center forwards the aggregated data access request to the data center with the *id* corresponding to the data receiver [5, 20].

3) After receiving $SAMDD^+$, the access control center calls $SPRE$ to convert the ciphertext and sends $SAMDD_{pk_j}$ to the specified data receiver.

4) The data receiver DR_j Calls $DPRE$ for decryption and gets the aggregated data M.

4.7 Data Processing

For Horner rule, the process is shown in **Algorithm 1**.

Algorithm 1 Horner recovery

1: Input: PM, R.
2: Output: The recovered sequence of values $(a_1, a_2, \cdots, a_l) X_0 \leftarrow \frac{PM}{R}$.
3: The plaintext M obtained by the data receiver satisfies Formula (14).

$$\begin{aligned} M = R_2^1 \sum_{j=1}^{l} R_1^j \sum_{k=1}^{n} d_{1kj} + \\ \cdots + R_2^m \sum_{j=1}^{l} R_1^j \sum_{k=1}^{n} d_{mkj} \end{aligned} \tag{14}$$

4: Marking $AM_{ij} = \sum_{k=1}^{n} d_{ikj}$, $AM_i = \sum_{j=1}^{l} R_1^j AM_{ij}$, $AM = \sum_{i=1}^{m} R_2^i AM_i$.
5: Take AM_i and R_2 as parameters, call algorithm 1, it can get $AM_1, AM2, \cdots, AM_m$.
6: After $m+1$ calls, all the results are available. The data receiver can then perform statistical analysis.

5 Security Analysis

Theorem 1. *The scheme proposed in this paper is correct. The proof is as follows.*

1) The encrypted data [11, 13, 17] and signature generated by user intelligent education Userk can satisfy Formula (7) and Formula (9) in the batch verification algorithm. The verification process is shown in Formula (15).

$$e(P, \sum_{D_{ir} \in Set_{i1}}) = \prod_{D_{ir} \in Set_{i1}} e(P, \sigma_{ir}). \tag{15}$$

Therefore, $RAGW_i$ is able to batch verify the authenticity and integrity of data D_{ik} from smart meters in the region.

2) The aggregated ciphertext and signature generated by $RAGW_i$ can be successfully checked, as shown in Formula (16).

$$e(P, \sum_{D_r \in Set_1}) = \prod_{D_r \in Set_1} e(P, \sigma_r). \tag{16}$$

Therefore, the data center can batch verify the authenticity and integrity of data D_i from different regions.

6 Security Attribute Comparison

This section makes a detailed comparison between the proposed scheme and ES-PPDA [1], FGPP [7] and CSDA [3] from the perspective of security attributes. In the previous scheme, users directly use the public key of the control center to encrypt, so the control center has the ability to decrypt user ciphertext directly. In this scheme, the joint key of data center and access control center is used for encryption, which avoids the direct decryption ability of a single entity in the system to obtain ciphertext. At the same time, this paper also uses proxy re-encryption technology to extend the control center to meet the demand of multi-data receiver scenario to access the aggregated ciphertext. In addition, for a specific legitimate data request, only the specified data receiver can

get the final aggregated data. Other entities, including the data center and the access control center participating in the proxy reencryption, can not get any information about the aggregated data, thus achieving fine-grained access control. The specific security attribute pairs are shown in Table 2.

Table 2: Security attribute comparison

Method	Privacy	Integrity	FG access control
Proposed	Yes	Yes	Yes
ES-PPDA	Yes	Yes	No
FGPP	Yes	Yes	No
CSDA	Yes	Yes	No

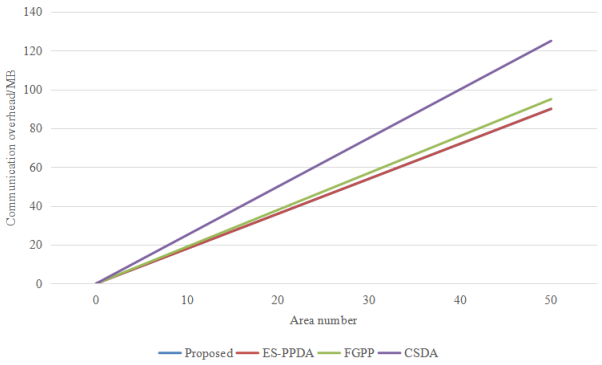


Figure 2: Comparison of the communication cost of users sent to the area aggregation gateway

7 Efficiency Analysis

7.1 Computational Overhead

In this section, the proposed scheme is compared in detail with ES-PPDA, FGPP and CSDA in terms of calculation cost. Because multiplication in $Z^*_{N^2}$ is relatively inexpensive compared to exponentials or bilinear pairings in $Z^*_{N^2}$, it can be ignored in comparison. Define C_e to represent the computational overhead required to perform an exponential operation in $Z^*_{N^2}$. C_m represents the computational overhead required to perform a multiplication in G_1. C_p represents the computational cost of a bilinear pairing operation. Assume that each user has l-dimension student information, each area has n_i users, and each area has a maximum of n users, there are m areas. Table 3 shows the computational cost of the proposed scheme and the related data aggregation scheme in each stage. As can be seen from Table 3, the proposed scheme has a good performance in terms of computational efficiency. And the number of exponential operations added to extend access control capabilities is constant, so the computational overhead of these additional operations is still low.

7.2 Communication Overhead

This section makes a detailed comparison between the proposed scheme and Scheme ES-PPDA, FGPP and CSDA in terms of communication cost. In the process of data transmission, the main data consists of three parts: user data ciphertext, other information (such as identity ID, time stamp, etc.) and signature.

1) Suppose $|N| = 1024$-bit, then Paillier cipher length is 2048-bit, and EDD cipher text is divided into two parts, each of 2048-bit, so the EDD ciphertext a total length of 4096-bit.

2) Assumption $|G_1| = 160$-bit, then the length of the BLS short signature for 160-bit.

3) Assume that the length of other information is the same in these scenarios, for example, the length of information is 100-bit.

4) Assume that i region has n_i users, each region has a maximum of n users, and there are m regions. The specific communication cost pairs are shown in Table 4. In order to more intuitively compare the communication cost differences between the proposed scheme and other relevant schemes, this paper assumes that each area has a maximum of 5000 users. The region number is the abscissa coordinate, the communication cost is the ordinate coordinate, and the communication efficiency of each scheme is compared. The comparison of the communication cost of users to the area aggregation gateway is shown in Figure 2. Figure 3 shows the communication cost comparison between the area aggregation gateway and the data center. The comparison of communication overhead from the access Control center to the data receiver is shown in Figure 4. As can be seen from FIG. 2 to FIG. 4, due to the use of EDD encryption system with long ciphertext length, the communication overhead of the proposed scheme increases by about one time. However, compared with the extension of fine-grained access control in function, the increase in communication overhead is still reasonable.

8 Conclusions

Previous data aggregation schemes cannot simultaneously meet the three security attributes of intelligent education, namely, privacy of user and student data, integrity of student data and fine-grained access control. This paper proposes for the first time a data aggregation scheme for privacy protection that can satisfy the three security attributes simultaneously. First of all, this paper uses the joint key to encrypt the user's student data, so that the data center and the access control center each have

Table 3: Computation cost comparison

Method	Proposed	ES-PPDA	FGPP	CSDA
User	$2C_e + C_m$	$2C_e + C_m$	$(l+1)C_e + C_m$	$2C_e + C_m$
RAGW	$(n_i+2)C_p$ $+(n-n_i)C_e + C_m$	$(n_i+2)C_p$ $+(n-n_i)C_e + C_m$	$(n+1)C_p + C_m$	$3nC_p + C_m$
DGM	$(m+2)C_p + C_m$	$(m+2)C_p + C_m$	—	—
Date center	$3C_e$	—	—	—
Access control center	$3C_e$	—	—	—
Data receiver	$4C_e$	$2C_p$	$2C_p$	$3mC_p$

Table 4: Communication overhead comparison/bit

Method	Proposed	ES-PPDA	FGPP	CSDA
$User \rightarrow RAGW$	4356mn	2307mn	2307mn	2467mn
$RAGW \rightarrow DGW$	4356mn	2307mn	—	—
$DCC \rightarrow ACC$	4096	—	—	—
$DGW \rightarrow CC$	4096	2308	2308	2467m

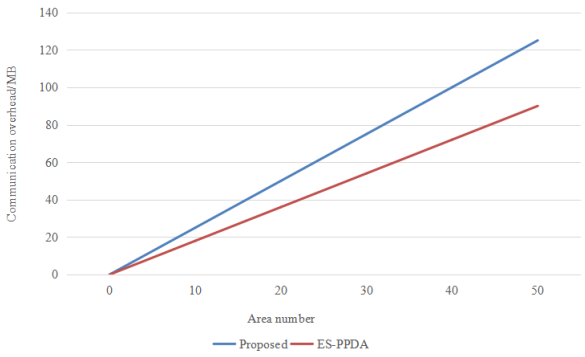


Figure 3: Comparison of the communication cost between the area aggregation gateway and the data center

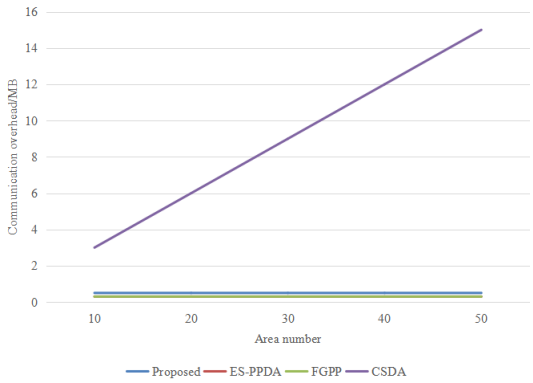


Figure 4: Comparison of communication overhead from access control Center to data receiver

part of the key, to ensure the privacy of the user's student data. Secondly, lightweight neural network is used to verify the integrity of data transmitted between entities. Finally, this paper introduces the proxy re-encryption scheme HERS, which co-works with the data center and the access control center to re-encrypt the aggregated ciphertext with the public key of the specified receiver, so as to achieve fine-grained access control. The next step is to explore a joint key processing approach that supports more key share holders, thereby providing greater resistance to colluded attacks between key share holders. At the same time, the parallelization of agent re-encryption stage will also be the key to improve the efficiency of scheme execution.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] Q. Chen, L. Wu, C. Jiang, "ES-PPDA: an efficient and secure privacy-protected data aggregation scheme in the IoT with an edge-based XaaS architecture," *Journal of Cloud Computing*, vol. 11, no. 1, pp. 1-12, 2022.

[2] J. Fan, B. Qin, F. Gu, Z. Wang, X. Liu, Q. Zhu, J. Yang, "Automatic Detection of Horner Syndrome by Using Facial Images," *Journal of Healthcare Engineering*, vol. 2022, 2022.

[3] W. Fang, X. Wen, J. Xu, J. Zhu, "CSDA: a novel cluster-based secure data aggregation scheme for

WSNs," *Cluster Computing*, vol. 22, pp. 5233-5244, 2019.

[4] P. Hu, Y. Wang, B. Gong, Y. Wang, Y. Li, R. Zhao, H. Li, B. Li, "A secure and lightweight privacy-preserving data aggregation scheme for internet of vehicles," *Peer-to-Peer Networking and Applications*, vol. 13, pp. 1002-1013, 2020.

[5] P. P. Jati, M. Reisen, E. Flikkenschild, F. Oladipo, B. Meerman, R. Plug, S. Nodehi, "Data access, control, and privacy protection in the VODAN-Africa architecture," *Data Intelligence*, vol. 4, no. 4, pp. 938-954, 2022.

[6] M. Kwet, P. Prinsloo, "The 'smart' classroom: a new frontier in the age of the smart university," *Teaching in Higher Education*, vol. 25, no. 4, pp. 510-526, 2020.

[7] H. Li, X. Li, Q. Cheng, "A fine-grained privacy protection data aggregation scheme for outsourcing smart grid," *Frontiers of Computer Science*, vol. 17, no. 3, pp. 173806, 2023.

[8] Y. Liu, W. Guo, C. Fan, L. Chang, C. Cheng, "A practical privacy-preserving data aggregation (3PDA) scheme for smart grid," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1767-1774, 2018.

[9] X. Lv, M. Li, "Application and research of the intelligent management system based on internet of things technology in the era of big data," *Mobile Information Systems*, vol. 2021, pp. 1-6, 2021.

[10] T. Rasa, A. Laherto, "Young people's technological images of the future: implications for science and technology education," *European Journal of Futures Research*, vol. 10, no. 1, pp. 1-15, 2022.

[11] S. Ravikumar, D. Kavitha, "IoT based home monitoring system with secure data storage by Keccak-Chaotic sequence in cloud server," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 7475-7487, 2021.

[12] Z. Sari, D. Chandranegara, R. Khasanah, H. Wibowo, W. Suharso, "Analysis of the Combination of Naïve Bayes and MHR (Mean of Horner's Rule) for Classification of Keystroke Dynamic Authentication," *Jurnal Online Informatika*, vol. 7, no. 1, pp. 62-69, 2022.

[13] B. Seth, S. Dalal, V. Jaglan, D. Le, S. Mohan, G. Srivastava, "Integrating encryption techniques for secure data storage in the cloud," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 4, pp. e4108, 2022.

[14] H. Shen, M. Zhang, J. Shen, "Efficient privacy-preserving cube-data aggregation scheme for smart grids," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 6, pp. 1369-1381, 2017.

[15] A. Singh, J. Kumar, "A secure and privacy-preserving data aggregation and classification model for smart grid," *Multimedia Tools and Applications*, vol. 82, pp. 22997-C23015, 2023.

[16] R. Wang, X. Li, C. Ling, "Pelee: A real-time object detection system on mobile devices," *Advances in neural information processing systems*, vol. 31, 2018.

[17] X. Wang, S. Yin, M. Shafiq, A. Laghari, S. Karim, O. Cheikhrouhou, W. Alhakami, H. Hamam, "A new V-net convolutional neural network based on four-dimensional hyperchaotic system for medical image encryption," *Security and Communication Networks*, vol. 2022, pp. 1-14, 2022.

[18] W. Winarno, A. Agoes, E. Agustin, D. Arifianto, "Ball detection for KRSBI soccer robot using PeleeNet on omnidirectional camera," in *AIP Conference Proceedings. AIP Publishing*, vol. 2314, no. 1, 2020.

[19] M. Yang, I. Tjuawinata, K. Y. Lam, T. Zhu and J. Zhao, "Differentially Private Distributed Frequency Estimation," *IEEE Transactions on Dependable and Secure Computing*, 2022. doi: 10.1109/TDSC.2022.3227654.

[20] Y. Zhang, S. Li, "Kinematic Control of Serial Manipulators Under False Data Injection Attack," *IEEE/CAA Journal of Automatica Sinica*, vol. 10, no. 4, pp. 1-11, 2023.

[21] D. Zheng, L. Meng, S. Yin, H. Li, "Enhanced Differential Private Protection Method Based on Adaptive Iterative Wiener Filtering in Discrete Time Series," *International Journal of Network Security*, vol. 23, no. 2, pp. 351-358, 2021.

Biography

Jian Zhang biography. Jian Zhang is with Zhengzhou Medical College. Research interests are Information security, Computing networks, Intelligent education.

Research on Anti-leakage Construction Data Encryption Algorithm Based on Generative Adversarial Networks and Symmetric Encryption

Yuping Peng[1] and Mingju Zhao[2]
(Corresponding author: Yuping Peng)
School of Civil Engineering and Architecture, Zhengzhou University of Science and Technology[1]
School of Electronic and Electrical Engineering, Zhengzhou University of Science and Technology[2]
Xueyuan Road, Mazhai Industrial Park, Erqi District, Zhengzhou City
Email: ancrum@qq.com
(Received Nov. 20, 2022; Revised and Accepted June 16, 2023; First Online June 25, 2023)
The Special Issue on Computational Intelligence Networks for Privacy and Security in Evolving Internet of Multimedia Things
Special Editor: Prof. Shoulin Yin (Harbin Institute of Technology)

Abstract

In the data storage process, privacy data leakage will occur. Generative Adversarial Networks (GANs) are a deep learning model. Through the confrontation with the discriminating model, the gradually perfect generating model is obtained to produce the data, which is hard to distinguish between true and false. A new research direction is to realize encryption algorithms by generating a countermeasure network. This paper proposes an anti-leakage encryption method based on GANs and symmetric encryption. This model can realize secure encrypted communication. Furthermore, the neural network models of communication partners and adversaries are improved by adding a complete connection layer, modifying activation function, and normalizing data batch. Through countermeasure training, the improved neural network model can realize secure communication of below 8 bits and key information leakage. Finally, experiment results show that the proposed encryption method has higher encryption effectiveness.

Keywords: Privacy data leakage; GANs; Anti-leakage encryption; Symmetric encryption

1 Introduction

The anti-leak cryptographic is developed with the side channel attack technique, and its main concern is how to design the safe password scheme that can resist the various side channel attacks, which can be used to eliminate the impact of secret information on the safety of the other people [8, 17, 22]. In 2016, Bhuiyan proposed a computational leak model against leak cryptography with ground-breaking significance [4]. The weak key leak model proposed by Zhao reduced the difficulty of constructing secure cryptographic schemes against weak key leak attacks [28]. Zhou *et al.* [29] proposed to select plaintext secure public key encryption scheme in the weak key leakage model, so that anti-leakage cryptography could be extended to more application scenarios. In recent years, domestic researchers have also focused on the security of cryptographic system in the case of continuous key leakage.

Generative Adversarial Networks (GANs) is composed of a generative model and a discrimination model [5, 10, 26]. Its core idea is to allow generative model and discrimination model to learn from each other, so that the generative model and discrimination model can be continuously enhanced in the process of confrontation. Finally, it can obtain the generative model with mixing the false with the genuine data. GANs has been widely used and achieved good results, it has the best application effect in the field of computer vision including image generation and segmentation, image style migration and so on. In addition, remarkable achievements have been made in information retrieval, text generation and other fields.

In 2016, Abadi in the Google Brain team conducted research on secure communication by using the GANs [1]. The encrypted communication model consisted of two neural networks (Alice and Bob) that communicated with each other and an eavesdropper neural network (Eve). When Alice was conducting encryption communication with Bob, it tried to restrict Eve from eavesdropping on the communication between Alice and Bob. In the process of training, Alice and Bob are trying to improve the complexity of encryption and decryption, while Eve tries to make his decryption results similar to the plaintext, improving the accuracy of decryption. Through combat training, an encrypted communication model that ensures

normal communication and resistance to eavespenetration.

This paper studies the problem of secure encryption communication in the case of part key leakage by using GANs. Therefore, our main contributions are as follows.

1) Firstly, the basic structure of the anti-leakage cryptography based on the GANs is proposed.

2) Then, using Alice and Eve in the 16-bit key symmetric encryption scheme, the model is able to implement secure encrypted communication when the 1 bit key is leaked. In the 16-bit symmetric encryption scheme, when Alice, Bob and Eve leak 1-bit key, the proposed model can basically achieve secure encrypted communication.

3) Furthermore, the neural network model of the communication parties and the enemy is improved in terms of adding full connection layer, modifying activation function and data batch normalization, etc. The improved neural network model can realize secure communication below 8 bits of key information leakage through combat training.

This paper is organized as follows: Section 2, we review the related works. Section 3, we present the GANs and encryption communication. Section 4, we describe the anti-leak encryption communication based on GANs. Section 5, we present the enhanced anti-leak encryption model based on GANs and experiments analysis. Section 6, we conclude this paper.

2 Related Works

Modern cryptography assumes that the user key is completely hidden from possible attack. However, in practice, some information about the key can be obtained from the secret key or the encryption system by side channel attack, such as time attack, power loss, cold start attack and spectrum analysis. Akavia *et al.* [2] introduced the concept of key leakage. Even if an attacker obtained part of the information from the key, but the encryption scheme was still semantically safe, it was called the safe of leak-resilient attack. To simulate a leak, assuming an attacker can access the leaky Oracle and gain output of any function about the key. Many researchers proposed targeted proposals. In [21], to solve the data sharing and key leakage challenges, attribute-based encryption (ABE) was used to achieve data sharing combined with searchable encryption (SE). Most of the existing attribute-based searchable encryption (SE) schemes were inefficient and not suitable for IoT devices because of the large amount of attributes and keys. The key-leakage problem was serious in practice which very little literature focused on it. In order to address both problems, it proposed a key aggregation searchable encryption (KASE) scheme based on the blockchain with auxiliary input (AI), which was capable of achieving secure data sharing on the encrypted data. To maintain the security of the blockchain system, the machine learning technique, which could detect smart Ponzi schemes automatically had recently received extensive attention. However, the existing method had potential target leakage and prediction shift problems when dealing with category features and calculating gradient estimates. Besides, they also ignored the imbalance and repeatability of smart contracts, which often caused the model to over-fit. So, Fan *et al.* [12] introduced a novel method for detecting smart Ponzi schemes in blockchain. Specifically, it first expanded the dataset of smart Ponzi schemes and eliminate the unbalanced dataset via data enhancement. Then, it leveraged ordered target statistics (TS) to handle the category features of smart contract without target leakage. Finally, it proposed an anti-leakage smart Ponzi schemes detection (Al-SPSD) model based on the idea of ordered boosting. Most of the works are based on users' check-in history and social network data to model users' personalized preferences for interest points, and recommend interest points through collaborative filtering and other recommendation technologies. However, in the check-in history, the multi-source heterogeneous information (including the position, category, popularity, social, reviews) describes user activity from different aspects which hides people's life style and personal preference. However, the above methods do not fully consider these factors' combined action. Considering the data privacy, it is difficult for individuals to share data with others with similar preferences. Liu *et al.*, [20] proposed a privacy protection point of interest recommendation algorithm based on multi-exploring locality sensitive hashing (LSH). This algorithm studied the POI recommendation problem under distributed system. This paper introduced a multi-exploring method to improve the LSH algorithm. On the one hand, it reduced the number of hash tables to decrease the memory overhead; On the other hand, the retrieval range on each hash table was increased to reduce the time retrieval overhead. Meanwhile, the retrieval quality was similar to the original algorithm. Data owners store the local private data with plaintext form in the cloud server. It is difficult to guarantee the data privacy and security. So data owners usually encrypt the local private data and upload it into cloud server. The traditional multi-keyword ciphertext retrieval methods cannot take both accuracy and security into consideration. Therefore, Wang *et al.* [23] proposed a modified homomorphic encryption method for multiple keywords retrieval. It could effectively solve the privacy leakage of search keywords problem. Faiz *et al.* [11] used particle swarm optimization technique to improve the encryption key. Particle swarm optimization algorithms (PSO) got their inspiration from the social behaviour of birds and were well known population-dependent meta-heuristic algorithms. But these methods aim at specific problems, the effect is better.

In the realistic environment, the adversary could gain partial information about decryption private key through various types of side channel attacks, Li *et al.* [18] for-

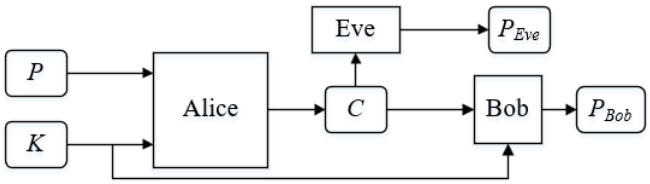


Figure 1: Alice, Bob and Eve in secure encrypted communications

malized a continuous leakage-resilient security model of certificate-based encryption. In the model, the adversary continuously obtained partial information about the secret states through the continuous leakage attacks. Furthermore, it constructed a continuous leakage-resilient certificate-based encryption scheme which was resilient to continuous leakage, and it was secure against adaptive chosen ciphertext attacks under the bilinear Diffie-Hellman inversion (BDHI) hardness assumption. Huang *et al.* [15] presented two generic constructions of continual leakage-resilient HPKE in the standard model by using a continual leakage-resilient all-but-one lossy trapdoor function. Xu *et al.* [25] proposed an efficient encryption scheme which was semantic secure in standard setting (i.e., without leakage) and could tolerate strong continuous leakage. It managed to construct such a secure scheme under strong leakage setting, by hiding partial ciphertext as secure as it hided the secret key using a small amount of more secure hardware resource, so that it was almost equally difficult for any adversary to steal information regarding this well-protected partial ciphertext or the secret key. It remarked that the size of such well-protected small portion of ciphertext was chosen to be much larger than the leakage threshold. It provided concrete and practical examples of such more secure hardware resource for data communication and data storage. Guo *et al.* [14] presented a certificate-based encryption resilient to continual leakage in the standard model. However, the above methods are not secure with a side-channel attack, attackers can obtain partial secret values of the schemes. So this paper proposes an anti-leakage encryption method based on GANs and symmetric encryption.

3 GANs and Encryption Communication

Coutinho *et al.* [9] designed both Alice and Bob and enemy Eve in the symmetric encryption system as neural network models, and realized secure encryption communication in the case of enemy monitoring through GANs. Its work begins with a classic cryptography scenario, as shown in Figure 1.

Alice conducts encryption communication with Bob. Alice uses the Key K to encrypt plaintext P and generate ciphertext C. Both Bob and Eve can obtain ciphertext C completely. Bob decrypts the ciphertext C through the

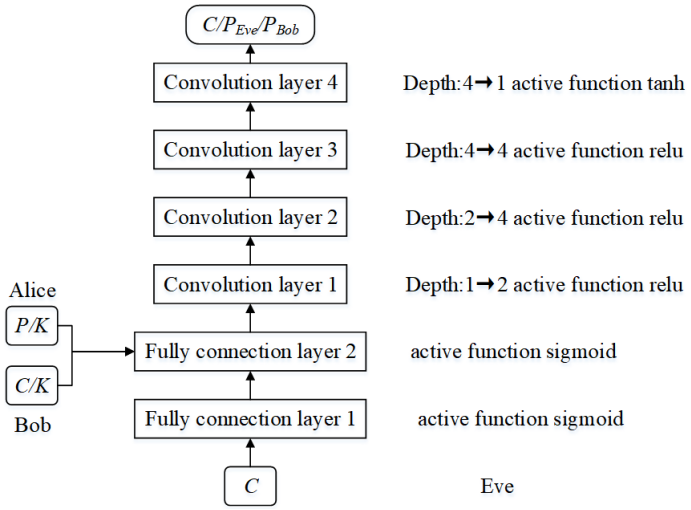


Figure 2: The neural network structure of Alice, Bob and Eve

key K, and gets the message P_{Bob} after decryption. Eve decrypts ciphertext C without any key to get the message P_{Eve}. The encrypted communication model composed by Alice and Bob and Eve's adversary model are constantly optimized in the process of confrontation training, so that the message P_{Bob} and plaintext P are exactly equal, while the difference between P_{Eve} and P is as large as possible.

Figure 2 shows the neural network model in which Alice and Bob models are the same, and Eve's neural network model adds a full connection layer to simulate the process of key generation. Alice inputs P and K and outputs encryption C. The inputs for Bob are C and K, and the decryption output is P_{Bob}. Eve as an adversary eavesdrops the information with input C and decryption output P_{Eve}. Alice and Bob jointly improve the encryption and decryption ability through training to ensure the decryption result $P_{Bob} = P$. Enemy Eve is trained to improve decryption and aiming at $P_{Eve} = P$. In practice, the loss rate of P_{Eve} is reduced to make P_{Eve} as close to P as possible. The antagonism between the communicator and the opponent is reflected in the mutual feedback during the training. Eve's training results are used for the next round of Alice and Bob's encryption and decryption training, and Alice and Bob's training results are used for Eve's next round of decryption training, so as to improve the security of encrypted communication scheme.

The experiment is carried out under the conditions of 16-bit plaintext and 16-bit symmetric encryption key. Through confrontation training, both communication parties can communicate normally, that is, $P_{Bob} = P$. The difference between Eve decryption results and plaintext remains 7-8 bits, that is, the decryption results are similar to the randomly generated results, and no more useful information is obtained.

In order to calculate the gap between the decryption results of Alice, Bob, Eve and the plaintext, the distance between the plaintext and the decrypted plaintext is given.

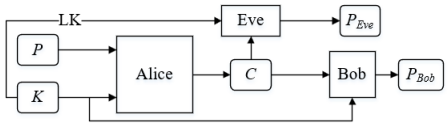


Figure 3: Anti-leak encryption communication scenario

Let N be the length of plaintext P and decrypted plaintext P_0, then the distance between P and P_0 is defined as:

$$d(P, P_0) = \frac{1}{N} \sum_{i=1}^{N} |P_i - P_{0i}|. \quad (1)$$

In Formula (1), since the per bit of plaintext randomly is as 1 or -1, $|P_i - P_{0i}|$ is 0 or 2, d is the average value of the difference bits between P and P_0. When P is exactly equal to P_0, $d = 0$, and when P is not exactly equal to P_0, $d = 2$. Given that P and P_0 only have -1 and 1, the difference between them has the greatest value when the $N/2$ bits are the same, and $d = 1$. Therefore, Eve's information loss is defined as the distance between P_{Eve} and plaintext P, as shown in Formula (2). Information loss $L_{Eve} = 1$ means Eve cannot decrypt the ciphertext and is in the state of random guessing.

$$L_{Eve} = d(P, P_{Eve}). \quad (2)$$

Because Bob and Alice need to resist Eve's decryption, the loss needs to involve Eve's loss L_{Eve} [27]. The information loss of the communicating party is denoted as L_{Bob}, and its calculation formula is defined as Formula (3).

$$L_{Bob} = d(P, P_{Bob}) + (L_{Eve} - 1)^2. \quad (3)$$

4 Anti-leak Encryption Communication Based on GANs

For the convenience of description, this paper first presents the anti-leak encryption communication system structure based on the GANs, as shown in Figure 3.

In Figure 3, Alice and Bob are the communicators. Alice uses the key K to encrypt the information P to generate ciphertext C. Bob accepts ciphertext C and decrypts data with key K to obtain plaintext P_{Bob} (regardless of symmetric encryption or asymmetric encryption, because the encryption and decryption keys are known). Eve is an enemy. He gets the ciphertext C and part of the leaked key LK, and uses them to decrypt the plaintext P_{Eve}. Alice, Bob and Eve are neural networks with the same computing power, because the communicators Alice and Bob have complete keys, so there is no doubt that normal communication can be achieved through neural network training. Eve steals ciphertext C and part of the key LK, and obtains many information through training. The goal of anti-leak encryption communication is to realize normal communication between Alice and Bob through neural network design and confrontation training, but Eve cannot get better decryption results than random guessing. In extreme cases, even if Eve gets 15 bits of the 16-bit key, the plaintext P cannot be decrypted and Alice, Bob still have normal communication.

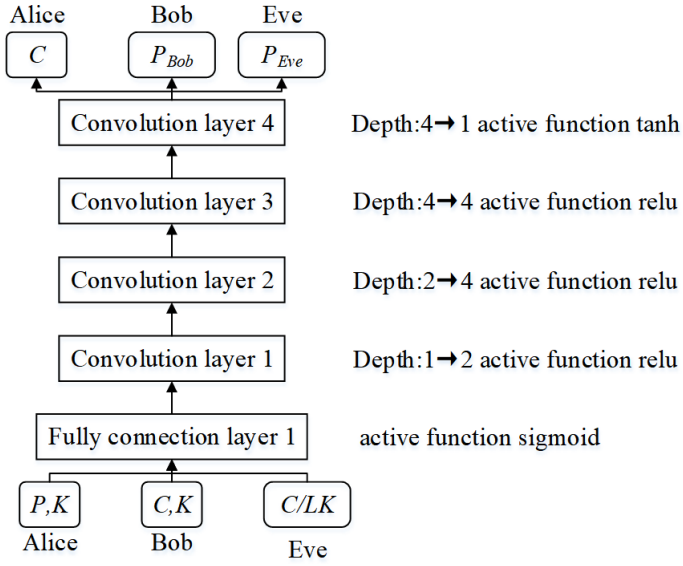


Figure 4: Preliminary anti-leak encryption communication model for Alice, Bob and Eve

This paper first uses the neural network model of Alice and Bob as shown in Figure 2. The connection layer 1 of Eve model in Figure 2 is used to speculate the key, but in this paper it has obtained a key leaking i bit in anti-leak encryption communication. Meanwhile, it is assumed that A,B,C have the same computing power. Therefore, it is assumed that Eve's neural network model is the same as Alice and Bob, and adding a new input for it, namely LK. The three-party neural network model is shown in Figure 4.

In this paper, the two sides of communication and the adversary are trained in the case of the key leakage of 1 bit and 2 bits. In their experiment, Alice, Bob and Eve all optimize their models using an Adam optimizer. Counter training is done in wheels. The learning rate of the model is set as 0.0008. Alice's input consists of plaintext P and key K. Bob's input consists of ciphertext C and key K. Eve's input consists of ciphertext C and part of the key LK. Where P, K, LK and C are represented by arrays with length N. Each bit in P and K is randomly assigned to -1 or 1. The n bits in the key K are randomly selected to generate part of the leaking key LK. n represents the number of bits with the same key, and the remaining bits are generated by random numbers. The following is the pseudo-code of the proposed model.

Alice network construction:

- Horizontal splicing of plaintext and key K as the input of Alice (supposing the length of plaintext and key is N).
- Alice inputs the $2N \times 2N$ fully connection neu-

ral network and outputs the activation function sigmnoid.

- The filter size of convolutional layer 1 is 4×1, the output network depth after scanning is 2, the step length is 1, and the activation function is Relu function.
- The size of the convolutional layer 2 filter is 2×2, the output network depth after scanning is 4, the step length is 2, and the activation function is Relu function.
- The size of the convolutional layer 3 filter is 1×4, the output network depth after scanning is 4, the step length is 1, and the activation function is Relu function.
- The size of the convolutional layer 4 filter is 1×4, the output network depth after scanning is 1, the step length is 1, and the activation function is tanh function.
- The output result is ciphertext C.

Bob network construction:

- Concatenating ciphertext C and key K as Bob's input (supposing the length of ciphertext and key is N).
- Bob inputs the $2N \times 2N$ fully connection neural network and outputs activation function sigmoid.
- The convolution network structure is exactly the same as that of Alice.

Eve network setup:

- The random bit in the key K is assigned to the leaked key K' as the leaking information. It generates other numbers by the random number and gets the leakage key K'.
- Ciphertext C and the leaked key $K'$are spliced as Eve's input.
- Eve inputs the $2N \times 2N$ fully connection neural network and outputs activation function sigmoid.
- The convolution network structure is exactly the same as that of Alice.

First, Alice and Bob are trained for encryption and decryption with 2000 times. After stabilization, Eve is trained for decryption by using the training results. The same training can achieve stabilization with 2000 times.

The next round uses Eve's decryption results to conduct encryption and decryption training for Alice and Bob, and then adopts the training results to conduct decryption training for Eve. A total of 10 rounds of training are conducted, and the training results are shown in Figure 5. The X-lable denotes the the number of Epoch, Y label denotes the loss percentage.

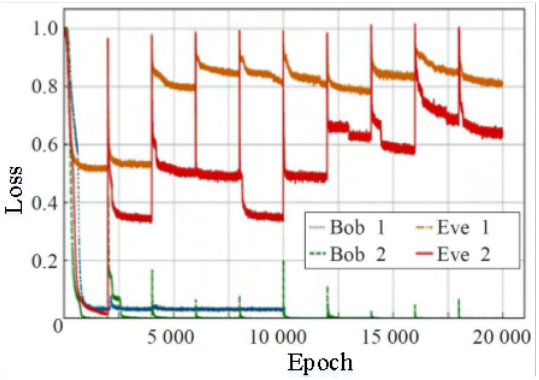


Figure 5: The anti-leak training results of the model

In Figure 5, when the 1-bit key is leaked, Alice and Bob can reach stability state after 5 rounds of training, and the information loss rate is close to 0. After 10 rounds of training, Eve's loss rate remains between 0.80 and 0.85, which is close to the best value. According to Equation (2), the correct bit number of Eve decryption accounts for about 40%-50% of the plaintext length, which is close to the correct bit of the random guess. This situation is compared with the original encrypted communication scheme without key leakage, Eve gets a little more information, but it still can not decrypt the information. When the two-bit key is disclosed, Alice and Bob can achieve stability after two rounds of training, which is faster than the one-bit key disclosure training. Eve can achieve stability after 10 rounds of training, but its information loss is stable between 0.6-0.7, that is, the correct decryption bit number accounts for about 30%-35%. Since the value of plaintext is only 1 and -1, this situation is equivalent to the proportion of correct decryption bit with 65%-70%. At this time, the leaked information is slightly bigger, which is no longer an acceptable anti-leak encryption communication scheme.

5 Enhanced Anti-leak Encryption Model Based on GANs and Experiments Analysis

The key of anti-leak encryption communication lies in partial key leakage, which not only guarantees the normal communication of Alice and Bob, but also guarantees that it cannot be correctly decrypted if Eve gets part of the key. As can be seen from the above experiment, the neural network model given by Abadi can barely be used when the 1-bit key is disclosed, but cannot be used when 2-bit or more are disclosed. Therefore, it cannot be directly used to solve the problem of anti-leak encrypted communication. In this paper, the model is improved from three aspects: improved activation function, enhanced neural network function and batch normalization.

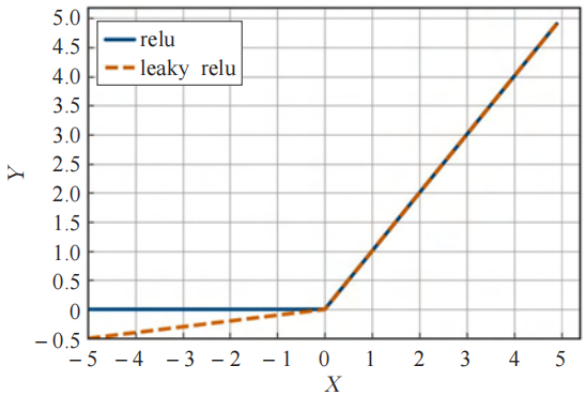


Figure 6: Relu and Leaky Relu activation function

5.1 Modified Activation Function in GANs

When the number of leaked keys increases, the loss of neural network model of Eve in Figure 4 decreases significantly, indicating that Eve is getting easier to decrypt the ciphertext. The using of Relu activation function in the model is likely to cause the death of neurons. According to the statistics of the dead neurons number in the model, the proportion of dead neurons in Alice and Bob is about 34%, and the proportion of dead neurons in Eve is 50%. The causes of death neurons have been pointed out in literature [7].

The specific reasons for modifying the activation function are given below. Figure 6 shows the Relu and Leaky Relu [7,19]. It can be seen from the figure that when the input of Relu function is negative, the output result is always 0, so the derivative of Relu function at the negative axis is also always 0. Because the weight update of neural network is realized through back propagation. The back propagation updates the weight by calculating the partial derivative of the loss E with respect to the weight w. When the output of the neuron is negative, the derivative of Relu must be 0, so the weight w will not be updated. For this reason, when multi-layer Relu neural network is used, many neurons tend to die, that is, most of the neurons no longer renew their weight, which represents the learning process stagnation of the neural network. This paper adopts the Leaky Relu function. Since the derivative of this function is not constant at the negative axis, it can effectively ensure that the partial derivative of E with respect to weight w is not always 0 when the input falls at the negative axis, and the weight can still be updated to avoid the stagnation of the learning process caused by the death of neurons. Therefore, all the convolutional neural networks in the model use Leaky Relu function, and the structure of the rest remains unchanged.

5.2 Enhancing the Complexity of the Model

Through the operation in the above section, the key leakage of secure communication is increased to 2 bits, the secure communication cannot be carried out. That is, neither Bob nor Eve can properly decrypt the ciphertext sent by Alice. This shows that the receiving network and the enemy network are confused by the encrypted information, the network decryption capacity reached the limit level. If the network model of Bob and Eve is enhanced, the decryption capability can be improved. But since Eve only has part of the key, its decryption capability is less than that of Bob. To verify this idea, the decryption capability of Bob and Eve is increased synchronously by adding a full connection layer to ensure the same decryption capability between Bob and Eve.

Model modification: Adding full connection layer 2 to the neural network model of Bob and Eve based on Figure 4. The activation function takes tanh function. The input and output remain unchanged. The input and output of Alice remain the same. At the same time, the activation function of the convolutional layer is modified to leaky Relu function.

Specific reasons for using tanh are given below. Figure 7 shows the derivative diagram of sigmoid and Tanh function. As can be seen from the figure, the range of the sigmoid derivative function is [0,0.25], while the range of the tanh derivative function is [0,1]. Since the derivative of sigmoid is at most 0.25, it is necessary to multiply a value less than or equal to 0.25 in the process of updating the weight and calculating the partial derivative. So the partial derivative is going to be smaller. As the layer number of sigmoid increasing, more numbers will be multiplied, which will become more and more serious and eventually lead to little weight updating. That is, the amount of back propagated information is greatly reduced, almost without any updating. Then there are many dead neurons, and the learning process will be stopped. The derivative of tanh used in this paper is greater than that of sigmoid [6,16]. Therefore, compared with sigmoid, the value of weight updating will not be compressed too small, and when the layer number of neural network increasing, the updating value will not be greatly affected.

Therefore, tanh can effectively slow down the phenomenon of dead neurons, thus avoiding the problem of stalled neural network learning process. Therefore, the activation function of full connection layer 2 takes tanh function instead of sigmoid.

5.3 Data Normalization Processing

Further analysis of the experimental results in section 4.2 shows that the stability of the model is improved after adding the full connection layer, but it is likely to fall into the local optimal position. Therefore, normalization processing is considered to reduce the influence of data difference factors on model optimization and improve the

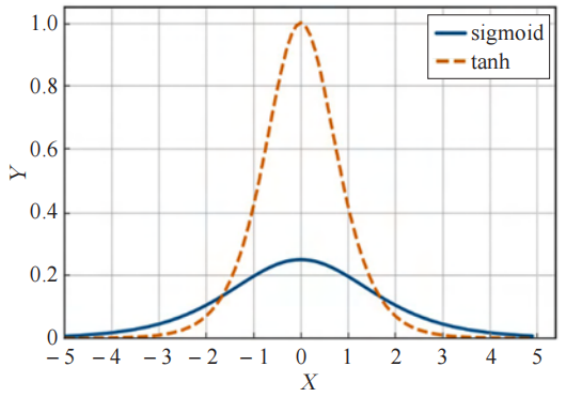


Figure 7: The derivative of sigmoid and tanh

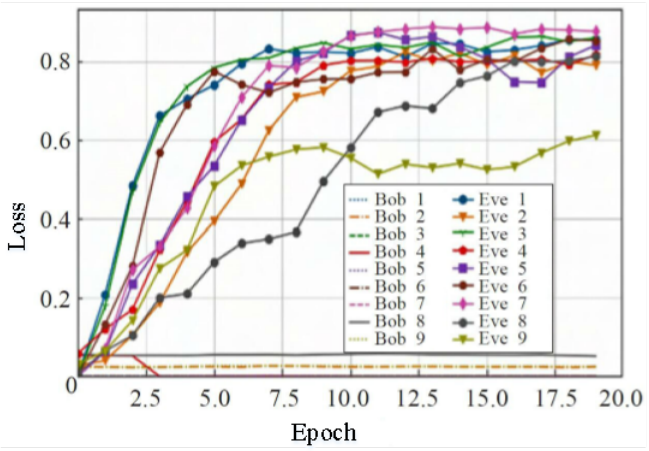


Figure 8: Results of 1-9 bit key leak

ability of neural network to find the optimal solution. Data scale normalization is to map the value range of data to a specific range in order to eliminate the influence of numerical attributes on the fairness of distance-based classification results due to their different size ranges. In this paper, input data of Bob and Eve model are processed by normalizing with mean value of 0 and variance of 1.

After data normalization processing, we conduct model training for 1-9 bit key leakage, the results are shown in Figure 8.

It can be seen from Figure 8 that the overall decryption ability of Bob and Eve has been greatly improved after the data normalization. Data normalization can further increase the stability of the model and avoid falling into local optimality. Bob's decryption ability can reach stability after 1-3 rounds of training, and the information loss is close to 0. Eve converges quickly in the case of 1 7 bit key leakage, and reaches a stable state after 9 rounds of training, the information loss can reach to 0.8. When the key leakage reaches to 8 bits, the convergence becomes slower, but the information loss is still around 0.8. However, when the key leakage reaches to 9 bits, the convergence is slow, and the stability is basically reached after 19 rounds of training, while the information loss is around 0.6. If the key leakage number continues to increase, a secure anti-leak encryption communication model cannot be obtained.

5.4 Time Analysis

We conduct eight encryption experiments. The average execution time of the algorithm is taken as shown in Table 1. We make comparison with LR-NIKE [13], LR-CKE [24], B-DKER [3].

Table 1: Time comparison

Method	Encryption time/s
LR-NIKE	0.712
LRCKE	0.687
B-DKER	0.667
Proposed	0.596

Through the time analysis, we can know that the proposed anti-leakage encryption method can obtain better results, the average time is 0.596s which is lower that that of other methods.

6 Conclusions

In this paper, the problem of anti-leak encryption communication is solved by using neural network and GANs, and the scheme of anti-leak encryption communication based on GANs is given. Based on Abadi's secure encryption communication model, through a series of experimental improvements, in the 16-bit symmetric encrypted communication environment, when the key leakage reaches to 8 bits, the secure anti-leak encryption communication model can be guaranteed. Our aims are to provide a new solution for anti-leak encryption communication, and prove the feasibility of the solution through experiments. However, the improvement of the neural network in this paper is only carried out from the aspects of increasing the complexity of the neural network, activation function and data normalization. The main method used is to improve the overall decryption ability and stability of the model. To counter leakage encryption communication problems, we can also start with more elaborate and targeted neural network structure, stronger encryption and decryption ability to increase the storage capacity of neural network model. It is expected that the ultimate goal of secure communication can be achieved by experiments in extreme cases where only rest 1 bit of key is not leaked.

References

[1] M. Abadi, B. Blanchet, C. Fournet, "The Applied Pi Calculus: Mobile Values, New Names, and Secure Communication," *Journal of the Association for*

Computing Machinery, vol. 65, no. 1, pp. 1.1-1.41, 2018.

[2] A. Akavia, S. Goldwasser, V. Vaikuntanathan, "Simultaneous Hardcore Bits and Cryptography against Memory Attacks," in *Reingold O. (eds) Theory of Cryptography. TCC 2009. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg*, vol, 5444, pp. 474-495, 2009.

[3] A. At, C. Ywb, "Revocable identity-based encryption with bounded decryption key exposure resistance: Lattice-based construction and more," *Theoretical Computer Science*, vol. 849, pp. 64-98, 2021.

[4] M. Bhuiyan, M. A. Hossain, J. M. Alam, "A computational model of thermal monitoring at a leakage in pipelines," *International Journal of Heat & Mass Transfer*, vol. 92, pp. 330-338, 2016.

[5] B. Bozorgtabar, D. Mahapatra, H. V. Teng, A. Poellinger, L. Ebner, J. P. Thiran, M. Reyes, "Informative sample generation using class aware generative adversarial networks for classification of chest Xrays," *Computer Vision and Image Understanding*, vol. 184, pp. 57-65, 2019.

[6] S. Chakraborty, J. Alawatugoda, C. P. Rangan, "New approach to practical leakage-resilient public-key cryptography," *Journal of Mathematical Cryptology*, vol. 14, no. 1, pp. 172-201, 2020.

[7] T. Y. Chang, M. S. Hwang, W. P. Yang, "A Communication-Efficient Three-Party Password Authenticated Key Exchange Protocol," *Information Sciences*, vol. 181, pp. 217-226, 2011.

[8] T. Y. Chang, M. S. Hwang, W. P. Yang, K. C. Tsou, "A Modified Ohta-Okamoto Digital Signature for Batch Verification and Its Multi-Signature Version," *International Journal of Engineering and Industries (IJEI)*, vol. 3, no. 3, pp. 75-83, 2012.

[9] M. Coutinho, D. Robson, F. Borges, L. J. Villalba, T. H. Kim, "Learning Perfectly Secure Cryptography to Protect Communications with Adversarial Neural Cryptography," *Sensors*, vol. 18, no. 5, 2018.

[10] S. U. Dar, M. Yurt, L. Karacan, A. Erdem, E. Erdem and T. Cukur. "Image Synthesis in Multi-Contrast MRI With Conditional Generative Adversarial Networks," *IEEE Transactions on Medical Imaging*, vol. 38, no. 10, pp. 2375-2388, 2019.

[11] M. Faiz, N. Fatima, R. Sandhu, M. Kaur, V. Narayan, "Improved Homomorphic Encryption for Security in Cloud using Particle Swarm Optimization," *Journal of Pharmaceutical Negative Results*, vol. 13, no. 10, pp. 4761-4771, 2022.

[12] S. Fan, S. Fu, H. Xu, X. Cheng, "Al-SPSD: Anti-leakage smart Ponzi schemes detection in blockchain," *Information Processing & Management*, vol. 58, no. 4, 2021.

[13] X. Gao, J. Mou, L. Xiong, Y. Sha, H. Yan, Y. Cao, "A fast and efficient multiple images encryption based on single-channel encryption and chaotic system," *Nonlinear Dynamics*, vol. 108, no. 1, pp. 613-636, 2022.

[14] Y. Guo, J. Li, M. Jiang, L. Yu, S. Wei, "Certificate-Based Encryption Resilient to Continual Leakage in the Standard Model," *Security and Communication Networks*, vol. 2020, no. 7, pp. 1-11, 2020.

[15] M. Huang, B. Yang, Y. Zhou, X. Hu, "Continual Leakage-Resilient Hedged Public-Key Encryption," *The Computer Journal*, vol. 65, no. 6, pp. 1574-1585, 2021.

[16] M. Lanza, A. Sebastian, W. Lu, M. Gallo, M. Chang, *et al.*, "Memristive technologies for data storage, computation, encryption, and radio-frequency communication," *Science*, vol. 376(6597), pp. eabj9979, 2022.

[17] H. Li, S. Yin, C. Zhao, L. Teng, "A Proxy Re-Encryption Scheme Based on Elliptic Curve Group," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 8, no. 1, pp. 218-227, 2017.

[18] J. Li, Y. Guo, Q. Yu, Y. Lu, Y. Zhang, F. Zhang, "Continuous leakage-resilient certificate-based encryption," *Information ences*, vol. 355, pp. 1-14, 2016.

[19] P. Li, Z. Chen, L. T. Yang, Q. Zhang, M. J. Deen, "Deep Convolutional Computation Model for Feature Learning on Big Data in Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 790-798, 2018.

[20] D. Liu, L. Shan, L. Wang, S. Yin, H. Wang, C. Wang, "P3OI-MELSH: Privacy Protection Point of Interest Recommendation Algorithm Based on Multi-exploring Locality Sensitive Hashing," *Frontiers in Neurorobotics*, vol. 15, 2021.

[21] J. Niu, X. Li, J. Gao, Y. Han, "Blockchain-Based Anti-Key-Leakage Key Aggregation Searchable Encryption for IoT," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 1502-1518, 2020.

[22] L. Teng, H. Li, "A high-efficiency discrete logarithm-based multi-proxy blind signature scheme," *International Journal of Network Security*, vol. 20, no. 6, pp. 1200-1205, 2018.

[23] X. Wang, S. Yin, H. Li, L. Teng, S. Karim, "A Modified Homomorphic Encryption Method for Multiple Keywords Retrieval," *International Journal of Network Security*. vol. 22, no. 6, pp. 905-910, 2020.

[24] J. D. Wu, Y. M. Tseng, S. S. Huang and T. T. Tsai, "Leakage-Resilient Certificate-based Key Encapsulation Scheme Resistant to Continual Leakage," *IEEE Open Journal of the Computer Society*, vol. 1, pp. 131-144, 2020.

[25] J. Xu, J. Zhou, "Strong leakage-resilient encryption: enhancing data confidentiality by hiding partial ciphertext," *International Journal of Information Security*, vol. 20, pp. 141-159, 2021.

[26] X. Yang, Y. Lin, Z. Wang, X. Li, K. Cheng, "Bi-Modality Medical Image Synthesis Using Semi-Supervised Sequential Generative Adversarial Networks," *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 3, pp. 855-865, 2020.

[27] S. Yin, H. Li, J. Liu, "A New Provable Secure Certificateless Aggregate Signcryption Scheme," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 6, pp. 1274-1281, 2016.

[28] Y. Zhao, X. Deng, C. H. Lee, H. Zhu, "Resettable Zero-Knowledge in the Weak Public-Key Model," in *International Conference on the Theory and Applications of Cryptographic Techniques*. vol. 2656, pp. 123-139, 2003.

[29] Y. Zhou, B. Yang, "Continuous Leakage-Resilient Public-Key Encryption Scheme with CCA Security," *Computer Journal*, vol. 60, no. 8, pp. 1161-1172, 2017.

Biography

Yuping Peng biography. Yuping Peng is with School of Civil Engineering and Architecture, Zhengzhou University of Science and Technology. Research interests are Information security, Computing networks.

Mingju Zhao biography. Mingju Zhao is with School of Electronic and Electrical Engineering, Zhengzhou University of Science and Technology. Research interests are Information security, Computing networks.

Swarm Model-based Computing Network for Economic Big Data Privacy Protection

Limin Chen

(Corresponding author: Limin Chen)

School of Finance and Economics, Zhengzhou University of Science and Technology
No. 1, Xueyuan Road, Mazhai Industrial Park, Erqi District, Zhengzhou, 450064
Email: chenwwencww@163.com

(Received Jan. 5, 2023; Revised and Accepted June 16, 2023; First Online June 25, 2023)

The Special Issue on Computational Intelligence Networks for Privacy and Security in Evolving Internet of Multimedia Things
Special Editor: Prof. Shoulin Yin (Harbin Institute of Technology)

Abstract

A data lake is the most commonly used data-sharing method for economic big data applications. However, the privacy problem brought by data sharing is still the missing part in the design of the data lake, mainly when applied to economic data confidentiality requirements are higher. The existing data lake design considers the data's characteristics to make the data-sharing platform more scalable and flexible. However, since the entire original data set is exchanged between peers who are not fully trusted, users using the data for analysis may redistribute the data shared by the data provider for profit without the prior consent of the data provider. To promote the circulation of valuable data, it is necessary to complete the missing data privacy of the existing data lake to share the data more securely across domains. To solve this problem, a data access and sharing model is proposed, and the Swarm model is optimized. The experimental results show that the purpose of data access control and security sharing can be realized by storing the hash value of data in the blockchain and using the trusted execution environment to store the original encrypted data in the data lake.

Keywords: Data Lake; Economic Big Data; Privacy Protection; Swarm Model

1 Introduction

With the continuous development of computer information technology, the performance of database system is becoming more and more powerful, the cost of data storage is decreasing, and people can get all kinds of information from more and more ways. Data mining is a key way to obtain useful knowledge from a large amount of information [11, 21]. However, in the process of mining valuable data, personal privacy data may be damaged. Data publishing is an important application direction of data mining. In real life, there are many places that need to publish data regularly. For example, some companies regularly publish quarterly financial statements, and hospitals release medical statistics. With the increasing amount of data released, attackers can lock individual privacy information through multiple data tables, leading to privacy leakage. Therefore, privacy protection has become an important issue [25].

At present, the traditional anonymous privacy protection model has been widely studied. The k-anonymous model [13] can make every record in the data table not be distinguished from other $k-1$ records, so that the attacker cannot identify the individual to which the private information belongs, thus protecting the privacy of individuals. The l-diversity model ensures that the probability of an attacker identifying a private record is less than $1/l$. However, such privacy protection models do not have a measure of the level of privacy and need to be constantly improved to defend against new attacks, such as background knowledge attacks and composite attacks [10]. In order to solve the above problems, Zhao *et al.* [27] proposed the differential privacy model, which caused a research boom. Differential privacy protection technology protects data by adding Laplacian noise so that the privacy leakage risk of data sets protected by differential privacy is controlled within an acceptable range.

In recent years, some research groups and scholars have carried out a lot of relevant research works on data privacy protection technology and achieved certain research results. In 2010, Ciriani *et al.* [3] proposed to combine data fragmentation with encryption, using fragmentation as a method to break sensitive associations between attributes to enhance the privacy of data collection. In 2020, Shah *et al.* [16] suggested using blockchain to decentralize data storage. However, this paper provides a complete implementation that uses the Swarm model to control access to data to defeat malicious attackers. In 2019, Liu *et*

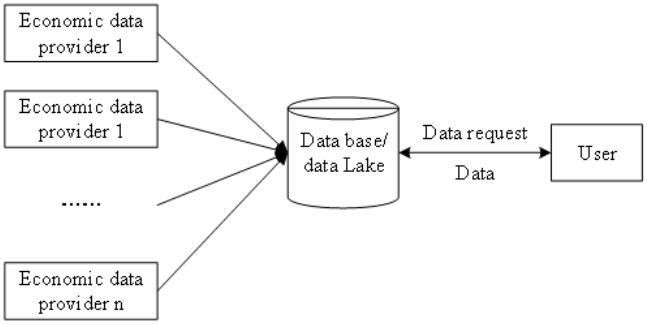


Figure 1: Economic data sharing mechanism in data lake

al. [14] suggested using blockchain to manage the Internet of Things by providing a lightweight blockchain consensus system where devices with low processing power could run the blockchain independently. In 2019, Chaaya *et al.* [2] proposed to build a privacy knowledge base that utilized the capabilities of the Semantic Web to determine how data consumers combined raw metadata to infer privacy-sensitive information and the privacy risks associated with disclosure of inferred information. In 2021, Zhang *et al.* [26] proposed a data security sharing method based on CP-ABE and blockchain to achieve fine-grained data sharing.

With the continuous construction and deepening of the application of economic informatization, various departments and businesses have been preliminarily integrated with informatization. The number and type of business data in the information system are increasing gradually, and the need for data sharing is urgent [1, 4]. At present, in our country's economic industry, there are few typical cases in which data chain, data governance and data services have formed landing platforms and provided services for enterprises. Although the economy has carried out informatization construction for many years, the location and magnitude of data storage are not clear. Structured data, unstructured data, real-time data, stream data and other data have not been effectively integrated, there are many independent applications among various departments, and the platform is not connected enough, which affects the development of data sharing and business integration. Secondly, the current data transmission protocol is not unified, how to carry out data storage by database and table, to achieve data center integration and transparent access has not been realized. Thirdly, it is urgent to analyze the storage value and application value of data, so as to establish the whole process inspection mechanism of data quality [17, 19]. The essence of data lake is a data management idea, which uses low-cost technology to capture, refine and explore the methods and technologies of large-scale and long-term original data storage. The data lake can store any kind of data, store data with high quality and efficiency, and process data faster and cheaper. The data sharing mechanism of the database is shown in Figure 1.

Smart contracts are autonomous applications that run within a blockchain. This paper constructs a data lake access management model through smart contracts, in which the rules of the interaction between data providers and data users are implemented independently in the blockchain network without centralized trust. Smart contracts provide users with the ability to control how data is accessed and used because smart contracts provide them with the same data management rights. By running these smart contracts using isolated virtual machines, users cannot modify the application results. Smart contracts and blockchains enable access control of data to track data usage between interested parties, thus enabling proper data access responsibility.

In this regard, this paper proposes a blockchain-based data access and control model and on this basis optimizes the swarm model in the blockchain, that is, it stores the hash value of data in the blockchain and uses the trusted execution environment to store the encrypted original data in the data lake. It not only solves the problems of difficult control of access rights within economic enterprises and difficult sharing of data between enterprises, but also ensures the security and privacy of sensitive data.

2 Related Works

2.1 Emergent Computation

Emergent Computation is a kind of innovative thinking logic that multi-agent systems show when dealing with complex problems. It is a system that uses multiple simple modules to communicate and collaborate with each other to spontaneously discover more complex behaviors. They occur in various fields of nature and society, such as fish, birds and ant colonies in nature, urban traffic flow, applause synchronization and complex network behavior in social fields [24].

2.2 Swarm Model

Swarm model is a model built on the basis of nature's swarm behavior to study the emergent behavior of systems. It is based on Reynolds' "Boids" theory. Each individual determines the next step according to the three basic rules of alignment, aggregation and separation. Finally, the individual will form a variety of different arrangements on the whole, that is, emergence behavior. The Swarm model simplifies the study of emergent patterns in complex systems. Gunji *et al.* [5] proposed a specific calculation method for relevant behaviors. Each Agent decides the direction and speed of the next moment according to the surrounding environment and behavioral parameters. Hansen *et al.* [7] applied a purely data-driven method to learn local interactions of homogeneous swarms through observation data and to generate similar swarming behaviour using the learned model. Yin *et al.* [23] used the two-row orbital elements density in-

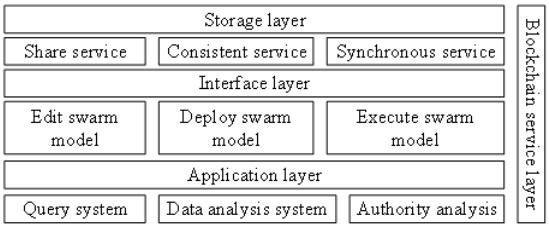


Figure 2: Data access and sharing model architecture based on blockchain

version to verify the atmospheric density accuracy results of the Swarm-C satellite accelerometer.

3 Data Access and Sharing Model

Data has become an important asset of enterprises. How to effectively control the access permission of data within enterprises and share data securely between enterprises and users is always a challenge. This paper proposes a data access and sharing model based on blockchain, which uses attribute-based encryption to control and share data access, so as to achieve the purpose of fine-grained access control and secure sharing. The characteristics of this model are as follows:

1) Use blockchain platform to provide decentralized data access management.

2) Use swarm model to provide the same data access management rights between users and data providers.

3) Use swarm model to provide complete system implementation on a real blockchain platform.

From the bottom to up, this model can be divided into storage layer, blockchain service layer, interface layer, swarm model layer, application layer, etc. Its architecture is shown in Figure 2.

1) Storage layer. The Trusted Execution Environment (TEE) is set up in the data lake to store original data. In addition, the Intel SGX architecture is used to implement trusted computing. The original data is encrypted and stored in the data lake for enterprise maintenance. Only the Hash address of the hashed data is stored in the blockchain.

2) Blockchain service layer. It is used to realize data consistency service and data synchronization service, and record the data interaction and sharing between enterprises and users.

3) Interface layer. It mainly includes data interface and swarm model interface.

4) The Swarm layer provides smart contract services. The main function is to provide data access control, that is, to authenticate the user who requests data, to confirm whether they have permission to access.

5) Application layer. It includes a variety of applications, such as data management system, data acquisition system, etc.

This model is mainly divided into two parts: data sharing within the enterprise and data interaction between the enterprise and the user. It is a parallel blockchain structure. Data sharing within the enterprise is mainly responsible for the storage and protection of data of various departments. In order to enhance the security and reliability of data within the enterprise, data is centrally managed and access permissions are limited [6]. The encrypted data is stored in a secure storage area, and only the hashed address of the data is stored on the chain. The storage structure is mainly divided into block header and block body. The input time stamp of the data, block length and Hash value of the previous block are taken as the block header. According to the access control tree, the data hash address, access control policy and data Merkle root are encrypted and packaged into blocks, stored in the block body, and then uploaded to the block chain.

The data interaction between enterprises and users will centrally process the collected user data for convenient sharing, and supervise the use of enterprise data. An access control tree generally adopts an attribute based encryption policy tree, and only specific departments in specific enterprises can decrypt it. When a data requester makes a data request, it is required to publish the requested data together with a token containing its own attributes to the corresponding blockchain.

During data storage, for a large number of underlying data and basic service data, asymmetric encryption will lead to confusion in key management. Therefore, attribute based encryption (ABE) is used to encrypt underlying data [12]. However, for sensitive data, due to the slow processing speed of blockchain, it is not suitable to store all data directly on the chain, so off-link storage is used. By creating a distributed hash table, the blockchain stores the hash address of the data. Data is encrypted when stored and data access is controlled through smart contracts. Table 1 compares this model with traditional blockchain in terms of data security and data storage.

4 Swarm Model Definition

In the Swarm model, agents interact with other individuals based on their own judgment in an environment where the group has no control center, thus affecting the whole. Similar to the agent in the Swarm model, any user in an economic enterprise can participate in functions such as publishing data, following interactions, commenting and liking, etc. Meanwhile, interactions between users also affect individual behaviors. According to the similarities between user interaction in economic topics and agent

Table 1: Comparison between proposed model and traditional blockchain

Compared type	Item	Advantages of proposed model	Traditional blockchain
Data security	Enterprise internal access control	ABE for fine-grained access control	not meet requirements
Data security	Hacking and data leakage	All the underlying data is encrypted	All data can be seen
Data storage	Data abuse	data requests are not feasible	Lack of effective access control
Data storage	Storage space utilization	Need to confirm request	All data is recorded on the chain

communication in the Swarm model, the key to integrating the swarm model into the user influence evaluation algorithm of economic topics is that the agent should flexibly combine users' behaviors such as releasing economic data, forwarding, commenting and liking in the process of movement.

Based on the calculation method in reference [18], the physical meaning of Swarm model is redefined here according to the research content of this paper. Before you give a definition, understand the following two concepts:

In the economic topic, user u_i neighbors the user node at time t. It refers to the set of users who have a great influence on user u_i, which is the set of users who forward user u_i microblog. The neighborhood users of user u_i are different at different times, which can be obtained according to the statistics of the user's forwarding network at the moment of microblog topic t.

In the microblog topic, user u_i is around the user node at the moment i. It refers to the set of users who have an influence on user u_i but not very much. It refers to the set of users who comment and like user u_i's microblog. Users around u_i are different at different times.

Swarm model for economic data topics

1) On behalf of an agent in Swarm model, V_1 points to the mean vector of all agents far from its own range d. In economic data, user u_i's neighborhood user node is used for calculation. The calculation formula is as follows:

$$V_{1t} = \sum_{v \in U} I_{t-1}(v) \times W_{1t}(vu_i). \quad (1)$$

$$W_{1t}(vu_i) = \frac{R_{1t}(vu_i)}{S_{1t}(vu_i)} \quad (2)$$

Where, U is the set of users participating in microblog topics. $I_{t-1}(v)$ is the influence of user v at one time. $W_{1t}(vu_i)$ is user u_i's contribution to user v's data forwarding at time t. $R_t(vu_i)$ is the number of microblog forwarding times between user v and user u_i at time t. $S_{1t}(vu_i)$ represents the total number of microblogs forwarded by all users at the time t when user v pairs the topic.

2) V2 is a vector pointing to the center of the simulated world in the Swarm model, which is represented by the average influence of the top 20% of users in the last iteration in the microblog user influence evaluation. The calculation formula is as follows:

$$V_{2t} = \frac{\sum_{v \in Top} I_{t-1}(v)}{n} \quad (3)$$

Top is the top 20% of users at the last moment. n indicates the number of Top users.

3) V_3 is the average velocity vector of all agents around an agent. Among microblog users, the average influence of user nodes around user u_i on users can be expressed. The calculation formula is as follows:

$$V_{3t} = \sum_{v \in U} I_{t-1}(v) \times W_{2t}(vu_i). \quad (4)$$

$$W_{2t}(vu_i) = \frac{D_t(vu_i)}{S_{2t}(vu_i)} \quad (5)$$

Where, $W_{2t}(vu_i)$ is user u_i's contribution to user v's data forwarding at time t. $D_t(vu_i)$ is the number of microblog forwarding times between user v and user u_i at time t. $S_{2t}(vu_i)$ represents the total number of microblogs forwarded by all users at the time t when user v pairs the topic.

4) V_4 is the vector that an agent points to the center formed by all agents around it. The calculation formula given in this paper is as follows:

$$V_{4t} = \frac{\sum_{v \in U} I_{t-1}(v)}{N} \quad (6)$$

N is the number of users in the topic.

5) V_5 is a random unit length vector, which is not taken into account in the calculation of Weibo users' behavioral influence.

The influence formula of user u_i at time t can be expressed as:

$$I_t(u_i) = c_1 \times V_{1t} + c_2 \times V_{2t} + c_3 \times V_{3t} + c_4 \times V_{4t}. \quad (7)$$

The development of an economic topic needs to go through the evolution cycle of germination, brewing, activation, climax and subside, which is similar to the emergent behavior of fish, birds and other groups in a complex system. Combining with the emergent computing model, this paper proposes a Swarm Model-user Rank (SMRank) algorithm based on the emergent computing swarm model. The algorithm first needs to calculate the initial value of user influence. Then calculate the influence of users at different times by iterating. Finally, it sums up the influence of users at different times to get the total influence value of users. The SMRank algorithm is described as shown in **Algorithm 1**.

Algorithm 1 SMRank algorithm

Input: Economic topic user participation network G, iteration number T;

Output: Total user influence $I(u_i)$;

1: Step 1. For user u_i, the initial value $I_0(u_i)$ of user influence is calculated according to Formula (**??**);
2: Step 2. For user u_i, it calculates user behavior influence $I_t(u_i)$ at time t according to Formula (7);
3: Step 3. $t = t + 1$; If t is less than T, go to step 2, otherwise go to step 4;
4: Step 4. For all users in the event, it uses the formula $I(u_i) = I_1(u_i) + I_2(u_i) + \cdots + I_T(u_i)$;
5: Step 5. Calculate the final user responsibility index $I(u_i)$, sort and output the result. The algorithm is complete.

5 Algorithm Design Descriptions

1) User registration. This module utilizes the user registration system on the Ethereum network. Each user joins the Ethereum network by generating a public private key pair that uniquely identifies the user and can then use the private key to interact with smart contracts to perform functions such as device registration and data access.

2) Register the device. Each authenticated data provider can be registered by providing an identifier for the data acquisition device. In smart contracts, this paper provides a Hash map to map the devices owned by the data provider to the owner address on the blockchain, such as mapping (address=list of owners device IDs).

3) Data write access policy. For a device writing data to the blockchain, the device will provide the owner address and device ID along with the data to be written. By using the combination of owner address and device ID as keys in the Hash map, you can uniquely store all data that corresponds to all devices, such as ((owner address, device id)=list of device data). The value of a Hash map is the Hash list of data written by the device. Before the smart contract allows data to be written to the contract, the smart contract checks that the owner address corresponds to the device ID to ensure that only the device owner can perform the write.

4) Device data read access policy. During data access, a user who needs to access device data needs to send a request permission to read data. The requesting user will provide the address and device ID of the device owner, including the Hash mapping of the device owner and address as well as the device ID as the user's key. For example, (owner address,device id,user address)=bool access). Finally, before granting access to the data, the hash map is checked to see if the requesting user can access the data by ensuring that only registered users can.

6 Experimental Analysis

6.1 Experimental Environment Configuration

A Trusted Execution environment (TEE) is built in the data Lake to store the raw data, and trusted computing is implemented using the Intel SGX architecture introduced in the new Intel Skylake processors [15]. By providing new instruction sets that extend the X86 and X86_64 architecture, user-level applications can provide confidentiality and integrity without the trust of the underlying operating system. At the same time, this experiment uses five different intelligent sensing devices to collect data and simulate the enterprise data acquisition device to write blockchain data to evaluate this algorithm. Experimental hardware is CPU 2.3 GHz Intel Core i5 16 GB 2133 MHz LPDDR3, GPU Intel Iris Plus Graphics 655 1536 MB. Experimental software is Python3.6 tensorflow1.13 pycharm [20].

6.2 Data Flow Analysis

Figure 3 shows a detailed data flow diagram of the experiment. For a device to write or read data, the device first registers itself using the blockchain while performing remote authentication services that enable users to trust the SGX platform. When performing a data write operation, the data provider should first retrieve the smart contract address, then encrypt and Hash the data, after hashing. The encrypted data is written to the blockchain via the WriteData() function in the smart contract and the original encrypted data is written to the SGX platform in the data lake. The integrity checking module then calculates the hashed based message authentication code (HMAC) of the data and writes the HMAC to the secure store along with the data.

For read operations, the user must register with the smart contract using the AllowAccess () method. To revoke access, the user can choose to execute the revokeAccess() function. The user can provide their address to

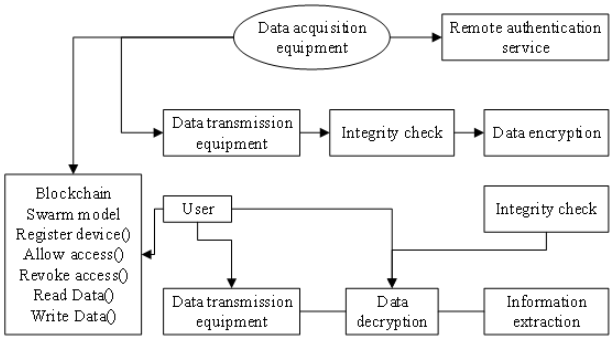


Figure 3: Data flowchart

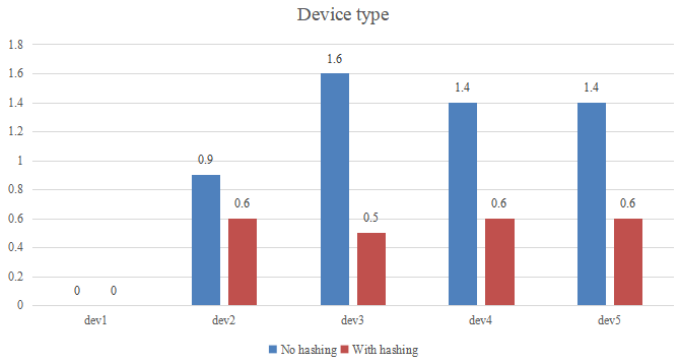


Figure 4: Gas usage for smart contract write operations

communicate with the smart contract, which checks if the user has access to the data and, if granted, returns a hash value for the data and can be used to access the data from the SGX storage platform. The SGX application then rechecks the smart contract using the READDATAAPI to determine if the user can access the data hash identifier. If access is allowed, the SGX application retrieves the data from the secure store. Note that the overhead of the blockchain read operation is irrelevant and will be shown later in the evaluation section of Table 2. Then it needs to decrypt the data and perform integrity checks to ensure the authenticity and integrity of the data. Finally, it needs to recalculate the HMAC of the data and compare it with the stored HMAC. If the HMAC has not changed, the data is read and returned to the user.

In addition, the attributes of the data set collected by the front-end intelligent sensor in this experiment can be roughly classified as shown in Table 2.

6.3 Experimental Results and Discussion

This experiment uses the Ethereum blockchain to implement the smart contract component, which mainly includes the reliability programming language. The code needs to be as concise as possible to limit the amount of Ethereum gas, or "gas", that fuels the Ethereum network world, needed to run smart contract transactions. It determines the normal operation of the Ethereum network ecosystem. When each write operation is executed on the chain, it needs to pay a certain fee. It is counted in the unit of gas, and each command that can be executed on the chain sets a gas value. At the same time, to limit the storage space needed to store the data, only the hash value of the data is stored in the blockchain. The experiment is evaluated by running smart contracts on the RinkebyEthereum test network. In this experiment, registerDevice, allowAccess, writeData, readData and revokeAccess are implemented so that the data acquisition device can interact with the smart contract. At the same time, this experiment uses the usage of Gas and throughput of blocks as evaluation indexes to conduct comparative analysis on whether to use Hash.

Table 3 shows the evaluation results of miners completing each smart contract operation. The data payload size of device 1 is 30B, device 2 is 50B, device 3 is 130 B, device 4 and 5 are 127B and 256 bit respectively. As shown in Table 3, registerDevice uses 47543 gas to complete its operation, allowAccess requires 29517 gas, writeData 51049 gas, revokeAccess 14792 gas, readData does not use any gas because the smart contract reading is done on the local blockchain, no mining is required.

In Figure 4, the amount of gas used by a miner to complete a write operation in the blockchain is compared. There are two scenarios, one is to write all encrypted data to the blockchain, and the other is to write only the Hash value of the data. Figure 4 shows that the data written by device 2 after hashing uses 59846 gas and 92926 gas for the original write, there is a 35% reduction. Device 3 uses 53454 gas to write the hashed data, compared to 159234 gas to write the original data, a 67% reduction. Devices 4 and 5 write hashed data using 58974 gas, while 140255 gas is required to write raw data, there is a 57% reduction.

Figure 5 shows the impact of increasing the write workload on the blockchain. Transaction throughput per second on the blockchain can be measured by increasing the write workload from 500 to 2000 write requests. Without hashing, the write transaction throughput is 10.56 writes per second for a 500 write workload. For 1500, it is 9.26, and for 2000 writes, the write throughput is 8.6 writes per second. With hashing, the write transaction throughput is 8.8 writes per second for a 500 write workload. For 1500, it is 7.9, and for 2000 writes, the write throughput is 7.2 writes per second. Write throughput decreases as the amount of write work increases, and decreases with the use of hashes. As can seen from Figure 4, gas usage with Hash is constant because the hash function generates 256 bits of data to be stored on the blockchain; Figure 5 shows that hashing before writing data to the blockchain can reduce write throughput.

The experimental results show that running smart contracts on the Ethereum test network for evaluation and only storing data hashes on the chain can reduce the gas usage of write operations and the throughput of the system on the basis of achieving access control.

Table 2: Data set attribute classification

Category	Corresponded attribute
Display identifier	name, ID, address
Standard identifier	age, workclass, race, sex, native_country
Sensitive information	relationship, occupation

Table 3: Application efficiency of smart contracts based on Gas consumption

Intelligent contract interface	parameter	Gas consumption
registerDevice	Device ID	47543
allowAccess	Device ID, ThirdParty address	29517
writeData	Device ID, DataHash	51049
readData	Device ID, ThirdParty address	—
revokeAccess	Device ID, ThirdParty address	14792

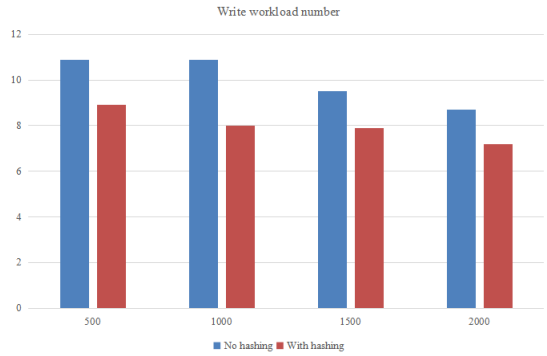


Figure 5: Increased throughput based on write effort

In this section, we compare encryption protection times with other methods including reference [9], reference [8], reference [22]. The results are shown in Table 4.

Table 4: Time consumption/s

State	[15]	[20]	[9]	Proposed
No hash	15.6	13.8	10.4	6.9
With hash	13.1	10.7	9.8	5.5

As can be seen from Table 4, the method in this paper has the shortest running time no matter in which state. Among them, with hash condition, the running time of the method in this paper reaches 5.5s, which has a great guarantee for data security.

7 Conclusion

With the continuous progress of information construction, the perfect data sharing and access control mechanism, data transmission transparency and data privacy are becoming more and more important. Based on the latest progress of blockchain technology, this paper proposes a data access and control model based on blockchain, and on this basis, the Swarm module of blockchain is optimized. Manage user access to data in a decentralized manner by utilizing blockchain, and ensure that all data processing and storage is done in a secure area. Storing original encrypted data in the data lake improves data security and integrity. The method proposed in this paper is helpful to realize the cross-business integration of enterprise data and provides a new technical solution to the major technical problems concerned by the construction of unified data center for economic enterprises.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] E. F. Cahyadi, T. W. Su, C. C. Yang, M. S. Hwang, "A certificateless aggregate signature scheme for security and privacy protection in VANET," *International Journal of Distributed Sensor Networks*, vol. 18, no. 5, 2022.

[2] K. B. Chaaya, M. Barhamgi, R. Chbeir, P. Arnould, D. Benslimane, "Context-aware system for dynamic privacy risk inference: Application to smart iot environments," *Future Generation Computer Systems*, vol. 101, pp. 1096-1111, 2019.

[3] V. Ciriani, S. D. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, P. Samarati, "Combining fragmentation and encryption to protect privacy in data storage," *ACM Transactions on Information and System Security*, vol. 13, no. 3, pp. 1-33, 2010.

[4] T. H. Feng, N. Y. Shih, M. S. Hwang, "Safety relay selection algorithms based on fuzzy relationship for wireless sensor networks," *The Journal of Supercomputing*, vol. 75, pp. 4601-4616, 2019.

[5] Y. P. Gunji, T. Kawai, H. Murakami, T. Tomaru, M. Minoura, S. Shinohara, "Lévy walk in swarm models based on Bayesian and inverse Bayesian inference," *Computational and Structural Biotechnology Journal*, vol. 19, pp. 247-260, 2021.

[6] I. Gupta, A. K. Singh, C. N. Lee, R. Buyya, "Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions," *IEEE Access*, vol. 10, pp.71247- 71277, 2022.

[7] E. Hansen, S. L. Brunton, Z. Song, "Swarm Modeling With Dynamic Mode Decomposition," *IEEE Access*, vol. 10, pp. 59508-59521, 2022.

[8] B. Jia, X. Zhang, J. Liu, Y. Zhang, K. Huang, Y. Liang, "Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 4049-4058, 2021.

[9] C. V. Joe, J. S. Raj, "Deniable authentication encryption for privacy protection using blockchain," *Journal of Artificial Intelligence and Capsule Networks*, vol. 3, no. 3, pp. 259-271, 2021.

[10] R. Khan, X. Tao, A. Anjum, T. Kanwal,S. R. Malik, A. Khan, W. Rehman and C. Maple, "θ-Sensitive k-Anonymity: An anonymization model for IoT based electronic health records," *Electronics*, vol. 9, no. 5, pp. 716, 2020.

[11] E. V. Kodirova, F. I. Mamurova, "Modern Methods of Teaching Information Technologies at the Lesson of Computer Science," *Pioneer: Journal of Advanced Research and Scientific Progress*, vol. 2, no. 3, pp. 86-89, 2023.

[12] H. Li, K. Yu, B. Liu, C. Feng, Z. Qin, G. Srivastava, "An efficient ciphertext-policy weighted attribute-based encryption for the internet of health things," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 5, pp. 1949-1960, 2021.

[13] C. Liu, Y. Tian, J. Xiong, Y. Lu, Q. Li, C. Peng, "Towards attack and defense views to k-anonymous using information theory approach," *IEEE Access*, vol. 7, pp. 156025-156032, 2019.

[14] Y. Liu, K. Wang, Y. Lin, W. Xu, "LightChain: a lightweight blockchain system for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3571-3581, 2019.

[15] B. McGillion, T. Dettenborn, T. Nyman,N. Asokan, "Open-TEE–an open virtual trusted execution environment," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, pp. 400-407, 2015.

[16] M. Shah, M. Shaikh, V. Mishra, G. Tuscano, "Decentralized cloud storage using blockchain," in *2020 4th International conference on trends in electronics and informatics (ICOEI'20)*, pp. 84-389, 2020.

[17] Z. A. Shaikh, A. A. Khan, L. Teng, A. A. Wagan, A. A. Laghari, "BIoMT modular infrastructure: The recent challenges, issues, and limitations in blockchain hyperledger-enabled e-healthcare application," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1-14, 2022.

[18] X. Wang, S. Yin, M. Shafiq, A. A. Laghari, S. Karim, O. Cheikhrouhou, W. Alhakami, H. Hamam, "A New V-Net Convolutional Neural Network Based on Four-Dimensional Hyperchaotic System for Medical Image Encryption," *Security and Communication Networks*, vol. 2022, pp. 1-14, 2022.

[19] M. M. Yang, I. Tjuawinata, K. Y. Lam, "K-Means Clustering With Local d_x-Privacy for Privacy-Preserving Data Analysis," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2524-2537, 2022.

[20] M. M. Yang, I. Tjuawinata, K. Y. Lam, J. Zhao, L. Sun, "Secure hot path crowdsourcing with local differential privacy under fog computing architecture," *IEEE Transactions on Services Computing*, vol. 15, no. 4, pp. 2188-2201, 2020.

[21] M. M. Yang, I. Tjuawinata, K. Y. Lam, T. Q. Zhu, J. Zhao, "Differentially Private Distributed Frequency Estimation," *IEEE Transactions on Dependable and Secure Computing*, 2022. doi: 10.1109/TDSC.2022.3227654.

[22] A. A. Yazdeen, S. R. Zeebaree, M. M. Sadeeq, S. F. Kak, O. M. Ahmed, R. R. Zebari, "FPGA implementations for data encryption and decryption via concurrent and parallel computation: A review," *Qubahan Academic Journal*, vol. 1, no. 2, pp. 8-16, 2021.

[23] L. Yin, L. Wang, W. Zheng, L. Ge, J. Tian, Y. Liu, B. Yang, S. Liu, "Evaluation of empirical atmospheric models using Swarm-C satellite data," *Atmosphere*, vol. 13, no. 2, pp. 294, 2022.

[24] B. Zhang, H. Li, S. Li, J. Peng, "Sustainable multi-depot emergency facilities location-routing problem with uncertain information," *Applied Mathematics and Computation*, vol. 333, pp. 506-520, 2018.

[25] D. Zhang, M. Shafiq, L. Wang, G. Srivastava, S. Yin, "Privacy-preserving remote sensing images recognition based on limited visual cryptography," *CAAI Transactions on Intelligence Technology*, 2023. https://doi.org/10.1049/cit2.12164

[26] Z. Zhang, X. Ren, "Data security sharing method based on CP-ABE and blockchain," *Journal of Intelligent & Fuzzy Systems*, vol. 40, no. 2, pp. 2193-2203, 2021.

[27] Y. Zhao, J. Chen, "A survey on differential privacy for unstructured data content," *ACM Computing Surveys (CSUR)*, vol. 54, pp. 1-28, 2022.

Biography

Limin Chen biography. Limin Chen is with School of Finance and Economics, Zhengzhou University of Science and Technology, Zhengzhou City, Henan Province,

450064, China. Her research interests are economic data security and business management.

An Efficient Homomorphic Deep Neural Network for Big Data Encryption Transmission Model in Internet of Vehicles

Junting Zhang

(Corresponding author: Junting Zhang)

School of Automobile, Henan College of transportation

Zhengzhou, 450000 China

Email: byoungholee@qq.com

(Received Jan. 5, 2023; Revised and Accepted June 16, 2023; First Online June 25, 2023)

The Special Issue on Computational Intelligence Networks for Privacy and Security in Evolving Internet of Multimedia Things

Special Editor: Prof. Shoulin Yin (Harbin Institute of Technology)

Abstract

The Internet of Vehicles (IOV) is a new generation of information and communication technology that enables all-round network connectivity referring to the realization of vehicles, pedestrians, and people (V2P), vehicles to vehicles (V2V), and Vehicle to infrastructure (V2I), Vehicle to network (V2N). IOV can improve the intelligence level of vehicles and autonomous driving ability, reduce the accident rate, improve traffic efficiency, improve car driving experience, build a new business form of automobile and traffic services, and provide users with intelligent, comfortable, safe, energy-saving, and efficient comprehensive services. In the networking of vehicles, the effect of big data encryption is not good because of the dynamic change of network topology. Therefore, we propose an efficient homomorphic deep neural network for the big data encryption transmission model in IOV. Considering the complex environment of the Internet of Vehicles, we mix homomorphic deep neural networks with encryption algorithms. A safe nonlinear calculation method is studied to avoid the multi-round iteration of ciphertext polynomial generated during the encryption model's construction and improve the nonlinear calculation's accuracy. This way, the corresponding nonlinear operator is implemented for the confused plaintext message, adding a random mask. Finally, the designed protocol's security, correctness, and efficiency are analyzed theoretically, and the effectiveness and superiority of the proposed model are verified experimentally.

Keywords: Big Data Encryption; Complex Environment; Homomorphic Deep Neural Network; Internet of Vehicles; Nonlinear Calculation

1 Introduction

The Internet of Vehicles can collect information such as the location and speed of vehicles and transmit the information to a central control center through the network. Through the intelligent department, the automatic management of vehicles can be realized, so that the data of the Internet of things can be widely used in automobile maintenance, automobile entertainment, finance and other fields [4, 24].

As the Internet of vehicles continues to expand, more and more data is generated. Traditional data transmission is based on a smaller and more centralized scale. For example, the big data transmission model of the Internet of Vehicles based on cloud edge fusion in reference [23] was based on the data fusion of the cloud edge grid. It used the decision engine to carry out big data analysis on the automobile network, and completed the safe transmission of big data according to the calculation results of similarity in an unified way. The big data transmission model of Internet of Vehicles based on blockchain protection proposed in reference [10] stored the big data of Internet of vehicles in a publicly distributed hash table and realized the safe transmission of big data according to the blockchain transaction signature and authentication process.

To solve the privacy leakage problem of data and neural network model assisted by cloud server, researchers have carried out a lot of research work by combining differential privacy, secure multi-party computing [1–3, 21], Homomorphic Encryption (HE) [12] and other technologies. This paper focuses on the research of neural networks for privacy protection based on homomorphic encryption. In terms of neural network-based privacy protection prediction, Ou *et al.* [16] theoretically analyzed the feasibility of approximate expression of nonlinear functions

by low-order polynomials, and proposed a dense neural network model based on Fully Homomorphic Encryption (FHE). The privacy protection prediction of neural network is realized. Malik *et al.* [14] used Taylor polynomial approximation to calculate nonlinear functions in neural networks, and introduced a Single Instruction Multiple Data (SIMD) mechanism to process encrypted data in parallel, which improved the efficiency of privacy protection prediction. In order to realize the privacy protection prediction of deep neural networks, Suma *et al.* [18] constructed a secure batch normalization layer based on BGV(Brakerski-Gentry-Vaikuntanathan)-FHE, and implemented a Rectified Linear Unit (ReLU) function by polynomial approximation. The proposed scheme was suitable for more complex image classification tasks. Al Kim *et al.* [11] improved a Brakerski-Fan-Vercauteren (BFV)-FHE scheme compatible with Graphics Processing Unit (GPU) settings. It provided theoretical conditions for the privacy protection neural network model to be applied in practice. Joye *et al.* [9] used TFHE (Torus Fully Homomorphic Encryption)-FHE and "self-start" technology to propose a privacy protection training scheme for binary neural networks under single server setting. In addition, Ye *et al.* [27] further realized the conversion between BFV ciphertext and TFHE ciphertext, used BFV ciphertext to calculate linear matrix multiplication and TFHE ciphertext to calculate nonlinear functions, constructed corresponding circuit modules, and completed the privacy protection training of neural network in hardware.

Xu *et al.* [22] proposed a blockchain-based sensitive data privacy-protection scheme for vehicles connected to the Internet. First, association rules were used to mine Big Data in the Internet of Vehicles. Then, a data security aggregation protocol was established. Finally, an end-to-end encryption mechanism was created. The privacy protection of Big Data in the Internet of Vehicles was achieved through static and dynamic strategies. Huang *et al.* [8] formalized a secure scheme for duplicated data that could prevent unnecessary storage and traffic on the cloud. This method ensured that an authorized intelligent connected vehicle (ICV) could logically outsource and retrieve data regardless of duplication. Wang *et al.* [20] proposed a Blockchain based Privacy-preserving Federated Learning scheme, which used blockchain as the underlying distributed framework of Federated Learning. He *et al.* [6] was to solve the problems in the communication security of intelligent transportation system (ITS) and improve the vulnerability of traditional distributed architecture. Although the above methods can independently complete the privacy protection model training on a single server, the scheme requires additional self-starting operations, and the non-linear function calculation depends on complex circuits, so the operation efficiency is still low.

Because there is a certain distance between the cloud server and the terminal device of the Internet of vehicles, although the above two methods can fully transmit data, they still face the security problems of information opacity and data leakage, which may lead to data loss or abuse by unauthorized users and cause infringement. Therefore, a big data encryption transmission model based on homomorphic deep neural network is proposed in this paper.

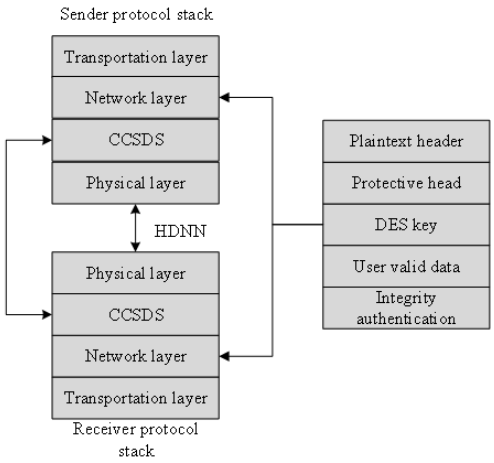


Figure 1: IOV big data encryption transmission module

2 Proposed Big Data Encryption Transmission Model for IOV

2.1 Constructing Big Data Encryption Transmission Model

Considering the complex environment of the Internet of vehicles, association rules and encryption algorithm are mixed to encrypt a large number of Internet of vehicles data, and then big data encrypted transmission model of Internet of vehicles big data based on homomorphic deep neural network (HDNN) is established, as shown in Figure 1.

As shown in Figure 1, key exchange and ID confirmation are needed for the encrypted transmission of big data on the Internet of Vehicles. The key exchange is the most important, which facilitates the transmission of big data on the Internet of vehicles. During data transmission, a virtual channel needs to be set up between the sender and the receiver to ensure data security [25, 26]. Big data encryption process of Internet of Vehicles, detailed process is as follows:

Step 1. The sender splits the data and adds it to a special protocol header wrapper. In order to achieve the purpose of data transmission protection, the security protocol data unit is designed in combination with HDNN, as shown in Figure 2.

Figure 2 shows that the security protocol data unit mainly consists of four parts: protocol plaintext header, protection header, user data, and integrity check threshold. The plaintext header consists of two

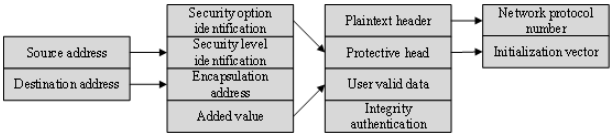


Figure 2: A protocol data unit based on HDNN

parts: the Internet protocol number and the initialization vector, which preserves the plain text during data transfer; The protection head encapsulates the source and target address of the communication system so as to achieve the purpose of information identification. The integrity check threshold, also known as the packet summary, is generally calculated using a hash function, then added to a valid data and wrapped [15].

Step 2. The sender encrypts data using the DES key and sends the data to the receiver. After receiving the key, the receiver performs packet processing and encrypts the data using the DES key to obtain plaintext information.

Big data that needs to be encrypted is counted. Assume that the $i-th$ measurement big data is g_i, and digital signature is performed on the data of Internet of vehicles:

$$K_i = f(C_i|T_i)^{sk_{ID_i}}. \tag{1}$$

Where, f represents the encryption hash function. C indicates ciphertext. sk indicates the output of the user private key. T_i represents the timestamp.

After the ciphertext, signature, and time stamp are sent to the gateway, the gateway needs to be authenticated. After receiving the ciphertext and signature pair sent by the Internet of Vehicles, Verify the identity of the Internet of vehicles through authentication. If the signature verification is correct, the gateway receives the ciphertext and signature uploaded to the Internet of Vehicles. Otherwise, the gateway refuses to receive the ciphertext and signature uploaded to the Internet of Vehicles.

After receiving the ciphertext and signature sent by the gateway, the bilinear group parameters are verified to be the same, so as to verify the identity of the gateway. The verification process is as follows:

$$\lambda(g, K) = \lambda(pk_{ID_\lambda}, H_\lambda(C_\lambda||T_\lambda)). \tag{2}$$

Where g stands for generator. If the signature sent by the gateway is correct, the car receives the ciphertext and signature stored on the gateway. Otherwise, the car rejects the ciphertext and signature. In this way, the big data used by the Internet of vehicles is obtained.

Step 3. The exchange of conventional data between vehicles is a common information, which is mainly accomplished by the communication between vehicles in the local area. To this end, encrypted big data is used for encrypted transmission.

In case of emergency, the emergency can be transmitted to vehicles in other areas through the traffic communication system, that is, the boundary node can directly transmit the emergency to the adjacent traffic node, and the emergency can be transmitted to the cloud server. The cloud server collaborates with a large amount of data to find the boundary nodes of other relevant areas, and transmits the emergency data to adjacent vehicle nodes through the edge nodes.

Step 4. The receiver receives the reply message and repeats Steps 1 to 3 until the complete data transmission is completed.

2.2 Homomorphic Deep Neural Network

The deep neural network is composed of input layer, hidden layer and output layer. Each layer contains several neurons, and each neuron is composed of five parts: input, weight, bias term, activation function and output. Without considering the activation function of neurons, the expression of neurons is reduced to linear regression equation. At this point, the whole network is only composed of multiple linear regressions, which can only solve the problem of linear separability. In order to solve the problem of linear indivisibility, activation functions, such as ReLU function and Softmax function [19], must be introduced. In general, the training process of fully connected neural networks can be divided into forward propagation and back propagation.

Forward propagation. The input data sequence passes through a number of fully connected layers and activation layers to obtain normalized classification probability output. The operation at layer l of the network can be described as $a^l = W^l x^{l-1}$, $x^l = f(a^l)$. Where a^l represents the neuron vector of layer l. W^l represents the weight matrix between the l and $l-1$ layers. x^{l-1} represents the output at layer $l-1$. b^l represents the l layer bias vector and f represents the activation function.

Back propagation. Back propagation calculates the derivative of target loss function with respect to model parameters according to the chain rule and completes the update of model parameters. If the cross entropy loss function $E = -\sum_j (label_j, lny_j)$ is used as the target loss function of the neural network, y represents the output of the neural network, $label$ represents the real label of the training sample. Back propagation first computes error $\delta^{l-1} = (W^l)^T \delta^l f'(a^l)$, and then updates model weight $\partial W^l = x^{l-1}(\delta^{l-1})^T$ and offset $\partial b^l = \delta^l$.

Where δ^l represents the error of layer l. ∂W^l and ∂b^l represent the gradient of weight and bias respectively. The update of gradient can be expressed as $W = W - \partial W^l \cdot \theta$, $b = b - \partial b^l \cdot \theta$. θ represents the learning rate.

2.3 BGV Homomorphic Encryption

BGV is a full-homomorphic encryption scheme based on Ring Fault-tolerant learning (RLWE) [17], which can support addition and multiplication homomorphism operations at the same time. The BGV encryption scheme includes the parameter setting algorithm $Setup$, the private key generation algorithm $SecretKeyGen$, the public key generation algorithm $PublicKeyGen$, the encryption algorithm Enc, and the decryption algorithm Dec.

1) $Setup(1^\lambda, u^\lambda)$. Based on the RLWE difficulty problem, the u bit cipher-text mode q and the plaintext mode p are selected, and the random parameters $d = d(\lambda, u)$, $n = n(\lambda, u)$, $N = N(\lambda, u)$ and $\chi = \chi(\lambda, u)$ are generated to satisfy the 2^λ bit safety. Output setup parameter $params = (q, p, d, N, n, \chi)$.

2) $SecretKeyGen(params)$. Let $t \leftarrow \chi^N$, output private key $sk \leftarrow (1, t[1], t[2], \cdots, t[n]) \in R_q^{n+1}$, where $R_q = Z_q[x]/(x^d+1)$ denotes polynomial quotient ring of module q.

3) $PublicKeyGen(params, sk)$. It uniformly generates the matrix $B \leftarrow R_q^{N \times n}$ and the vector $e \leftarrow \chi^n$, where $sk[0] = 1$, $t \in R_q^{n+1}$. Let $b \leftarrow Bt + pe$, public key pk consists of column b and matrix B.

4) $Enc(params, pk, m)$. Given the plaintext message $m \in R_p$, let $m = (m, 0, \cdots, 0) \in R_q^{n+1}$, take $r \leftarrow R_p^N$, the encrypted message is $c = m + A^T r \in R_p^{n+1}$.

5) $Dec(params, sk, c)$. Known ciphertext message $r \in R_p^{n+1}$, the encrypted plaintext message is $m = [[< c, s >]_q]_p$.

The BGV encryption scheme supports two Multiplication operations [28]: Plaintext-Cipher Multiplication (PCM) and Cipher-Cipher multiplication (CCM). The specific definition is as follows. In BGV scheme, the ciphertext is represented by a polynomial of order n, the ciphertext module is p, the computational complexity of PCM is $O(pn)$, and that of CCM is $O(p^2n^2)$.

Definition 1. *Given plaintext message m_1, and m_2, c_2 represents the ciphertext message of m_2. If homomorphic operation $\odot$ satisfies $c_2 \odot m_1 = Enc(m_1 \cdot m_2)$, homomorphic operation $\odot$ is called PCM operation.*

Definition 2. *Given plaintext message m_1, and m_2, c_1 and c_2 represent the ciphertext messages of m_1, and m_2 respectively, if the homomorphic operation $\otimes$ satisfies $c_2 \odot c_1 = Enc(m_1 \cdot m_2)$, the homomorphic operation $\otimes$ is called CCM.*

3 Experiment and Analysis

Automotive networks include mobile on-board terminals such as communications equipment, roadside infrastructure, certification centers, etc. TA is a trusted and authoritative automotive network security center.

In this paper, the deep neural network is taken as an example. The normalized classification probability is obtained by inputting k-dimensional data through two layers of FC, one layer of ReLU and one layer of Softmax, i.e., $k \rightarrow (FC_1 + ReLU) \rightarrow m \rightarrow (FC_2) \rightarrow t \rightarrow (Softmax) \rightarrow t$. HDNN can be divided into safe forward propagation and safe back propagation processes. Suppose Add represents a homomorphic addition/subtraction operation, $CMult$ represents a CCM operation, $PMult$ represents a PCM operation, Enc represents a encryption operation, and Dec represents a decryption operation. The computational complexity of the security forward propagation process is shown in Table 1. The secure FC layer uses SFMP protocol to convert $CMult$ operation into $PMult$ operation of low complexity, and the Add operation is used to complete the addition operation between neuron features. The secure ReLU layer and the secure Softmax layer require server S, which AIDS decryption and encryption and requires a small number of Ene and Dec operations to be performed. In addition, because the number of ciphertext multiplication in the nonlinear layer is small, $CMult$ operation is chosen to be performed directly.

Table 1: Computational complexity of secure forward propagation

Layer	$PMult$	$CMult$	Add	Enc	Dec
FC_1	km	0	$(k+1)m$	0	0
ReLU	0	$3m$	m	m	m
FC_2	mt	0	$(m+1)t$	0	0
Softmax	0	$3t$	$2t$	$5t$	$2t$

Assuming n represents the small batch size of the HDNN training, the computational complexity of the secure back-propagation process is shown in Table 2. For the back propagation of the secure Softmax layer, a small amount of Add is required to complete the subtraction operations of normalized features and sample labels. For the secure FC layer, $PMult$ is required to complete some multiplication operations. For the secure ReLU layer, no additional operations are required if the output symbol ciphertext is recorded during forward propagation.

Since HDNN scheme is built based on SFMP, SRP, SREP and SEP protocols, this paper mainly analyzes the communication rounds and communication overhead of these basic security protocols. Assuming that the unit plaintext size in the plaintext space is $||P||$ and the unit ciphertext size in the ciphertext space is $||C||$, the communication complexity of secure computing protocols is shown in Table 3. In the SFMP protocol, S_1 needs one

Table 2: Computational complexity of secure back propagation

Layer	$PMult$	$CMult$	Add	Enc	Dec
FC_1	$t(m+n)$	m	mt	0	0
FC_2	mn	0	0	0	0
Softmax	0	0	t	0	0

round of communication to share a random mask k with S_2, and the encrypted confused message $temp$ after the mask is added needs to be passed to S_3. S_3 can decrypt the obfuscated plaintext message and send the two encryption copies tw_1 and tw_2 to S_1 and S_2. The protocol requires four rounds of communication and the communication overhead is $3||P|| + ||C||$. Similar to SFMP protocol, SRP, SREP and SEP protocol also includes three stages: S_1 and S_2 share random mask, S_1 and S_2 send encrypted confused messages to S_3, and S_3 sends back encrypted share.

Table 3: Computational complexity of secure back propagation

Protocol	S_1+S_2	S_1+S_3	S_3+S_2	Message size
SFMP	1	2	1	$3\|\|P\|\| + \|\|C\|\|$
SRP	1	2	2	$\|\|P\|\| + 5\|\|C\|\|$
SREP	1	2	2	$\|\|P\|\| + 4\|\|C\|\|$
SEP	1	2	2	$\|\|P\|\| + 4\|\|C\|\|$

The security of HDNN scheme depends on the encryption security strength of BGV homomorphic encryption scheme, which is related to the bit length of the security parameter. N3 network is selected. Table 4 shows the training time results of HNN schemes for single batch with different bit lengths. With the increase of bit length, the increase of calculation module will lead to the increase of training running time. On the other hand, because the increase of ciphertext space will reduce the probability of random ciphertext recognition, the privacy protection intensity of HNN scheme will also be enhanced. Therefore, it is necessary to consider the security strength and efficiency of homomorphic encryption in the design of HDNN scheme.

Table 4: Comparison of HDNN training time with different bit lengths

Bit length	Running time/s
80	148
128	220
176	431

The FC layer involves a large number of homomorphic ciphertext multiplication operations. The SFMP protocol proposed in this paper converts CCM operations into PCM operations of low complexity. Table 5 shows the calculation cost comparison of CCM and PCM operations under different multiplication depths. The calculation cost of CCM and PCM increases with the increase of multiplication depth, which represents the number of times that BGV encryption schemes perform continuous multiplication without causing calculation errors, and is positively correlated with the modulus length of ciphertext space, which also means that each ciphertext message occupies longer bits, and the calculation cost of single multiplication is larger. Under the same multiplication depth, the computational cost of PCM is only about 10% of that of CCM, indicating that SFMP protocol can greatly improve the computational efficiency of privacy protection neural networks.

The privacy protection neural network training scheme ensures the privacy and security of data and models, but inevitably reduces the training efficiency. Three neural network models, N1, N2 and N3, were adopted for the experiment, and privacy protection training was performed on a group of small batch samples. The calculation cost of HDNN scheme and related schemes is shown in Table 6.

The PPML scheme based on dual server architecture uses CCM arithmetic to perform homomorphic ciphertext multiplication of features and parameters in FC layer, while the HDNN scheme in this paper uses SFMP protocol to convert CCM arithmetic into PCM arithmetic, which improves the computational efficiency of FC layer and saves 94.7% of training time. FHESGD and Glyph schemes not only use CCM operation to perform homomorphic ciphertext multiplication, but also use a single server to complete the neural network training process. Additional "self-starting" operation is required to compress and encrypt the multiplication noise, so as to ensure the correctness of homomorphic calculation. In contrast, the HDNN scheme sacrifices a small amount of communication overhead and makes the server S_3 execute the corresponding nonlinear operator for the obfuscated plaintext message, which can not only achieve accurate nonlinear computation, but also greatly reduce the computation overhead of single server ciphertext. In N2 network, the calculation cost of training 192 samples in batches by HDNN scheme is much lower than that of FHESGD scheme. Similarly, in N3 network, the computing cost of training single sample in HDNN scheme is only 2% of that in Glyph scheme.

4 Conclusions

Faced with the security problem of data transmission in Internet of vehicles, this paper proposes a big data encryption transmission model based on HDNN. This model combines a dynamic Byzantine protocol to achieve fault-tolerant consistency and secure encrypted transmission

Table 5: Comparison of computing cost between CCM and PCM

Depth of multiplication	PCM/ms	CCM/ms	Multiple
3	3.61	41.2	11.5
5	11.02	98.9	9.1
7	12.11	123.9	10.3
9	13.81	150.2	10.9

Table 6: The calculation cost comparison of different schemes

Network	Scheme	Batch size	Batch sample time/10^3s	Single sample time/s
N1	PPML [7]	192	10.471	54.56
N1	HDNN	192	0.551	2.89
N2	FHESGD [5]	60	118.001	1966.01
N2	HDNN	192	0.119	0.62
N3	Glyph [13]	60	2.901	48.34
N3	HDNN	192	0.221	1.142

of big data. The experiment and analysis show that the proposed model not only has a good delay control ability, but also has a good improvement in throughput capacity. The model can adapt to engineering practice well in efficiency, function, safety and other aspects, and has a good application prospect.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] E. F. Cahyadi, C. Damarjati, M. S. Hwang, "Research on identity-based batch verification schemes for security and privacy in VANETs", *Journal of Electronic Science and Technology*, vol. 20, no. 3, pp. 1-19, 2022.

[2] E. F. Cahyadi, M. S. Hwang, "A comprehensive survey on certificateless aggregate signature in vehicular ad hoc networks", *IETE Technical Review*, vol. 39, no. 6, pp. 1265-1276, 2022.

[3] E. F. Cahyadi, M. S. Hwang, "An improved efficient anonymous authentication with conditional privacy-preserving scheme for VANETs", *Plos One*, vol. 16, no. 9, 2021.

[4] J. Contreras-Castillo, S. Zeadally, J. Guerrero-Ibanez, "Internet of vehicles: architecture, protocols, and security," *IEEE internet of things Journal*, vol. 5, no. 5, pp. 3701-3709, 2017.

[5] S. Halevi, V. Shoup, "Design and implementation of HElib: a homomorphic encryption library," *Cryptology ePrint Archive*, 2020. (`https://ia.cr/2020/1481.`)

[6] Y. He, M. Kong, C. Du, D. Yao, M. Yu, "Communication Security Analysis of Intelligent Transportation System Using 5G Internet of Things From the Perspective of Big Data," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 2199-2207, 2023.

[7] E. Hesamifard, H. Takabi, M. Ghasemi, C. Jones, "Privacy-preserving machine learning in cloud," in *Proceedings of the 2017 on cloud computing security workshop*, pp. 39-43. 2017.

[8] D. Huang, J. Zhou, B. Mi, F. Kuang, Y. Liu, "Key-based data deduplication via homomorphic NTRU for internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 1, pp. 239-252, 2023.

[9] M. Joye, "SoK: Fully homomorphic encryption over the [discretized] torus," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 661-692, 2022.

[10] O. Kaiwartya, A. Abdullah, Y. Cao, A. Altameem, M. Prasad, C. T. Lin, X. Liu, "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects," *IEEE access*, vol. 4, pp. 5356-5373, 2016.

[11] A. Kim, Y. Polyakov, V. Zucca, "Revisiting homomorphic encryption schemes for finite fields," in *Advances in Cryptology-ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part III 27. Springer International Publishing*, pp. 608-639, 2021.

[12] C. Lan, H. Li, S. Yin, L. Teng, "A New Security Cloud Storage Data Encryption Scheme Based on Identity Proxy Re-encryption," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 804-810, 2017.

[13] Q. Lou, B. Feng, G. Fox, L. Jiang, "Glyph: Fast and accurately training deep neural networks on en-

crypted data," *Advances in Neural Information Processing Systems*, vol. 33, pp. 9193-9202, 2020.

[14] J. Malik, S. Kiranyaz, M. Gabbouj, "Self-organized operational neural networks for severe image restoration problems," *Neural Networks*, vol. 135, pp. 201-211, 2021.

[15] N. Mouha, M. Raunak, D. Kuhn, R. Kacker, "Finding bugs in cryptographic hash function implementations," *IEEE transactions on reliability*, vol. 67, no. 3, pp. 870-884, 2018.

[16] W. Ou, J. Zeng, Z. Guo, W. Yan, D. Liu, F. Stelios, "A homomorphic-encryption-based vertical federated learning scheme for rick management," *Computer Science and Information Systems*, vol. 17, no. 3, pp. 819-834, 2020.

[17] B. Rouabah, H. Toubakh, M. Kafi, M. Sayed-Mouchaweh, "Adaptive data-driven fault-tolerant control strategy for optimal power extraction in presence of broken rotor bars in wind turbine," *ISA transactions*, vol. 130, pp. 92-103, 2022.

[18] M. Suma, P. Madhumathy, "Brakerski-Gentry-Vaikuntanathan fully homomorphic encryption cryptography for privacy preserved data access in cloud assisted Internet of Things services using glowworm swarm optimization," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 12, pp. e4641, 2022.

[19] L. Teng, H. Li, S. Yin, "Im-MobiShare: An improved privacy preserving scheme based on asymmetric encryption and bloom filter for users location sharing in social network," *Journal of Computers*, vol. 30, no. 3, pp. 59-71, 2019.

[20] N. Wang, W. Yang, X. Wang, L. Wu, Z. Guan, X. Du, M. Guizani, "A blockchain based privacy-preserving federated learning scheme for Internet of Vehicles," *Digital Communications and Networks*, 2022. Doi:10.1016/j.dcan.2022.05.020.

[21] Y. Wu, X. Wang, W. Susilo, G. Yang, Z. Jiang, S. Yiu, H. Wang, "Generic server-aided secure multiparty computation in cloud computing," *Computer Standards & Interfaces*, vol. 79, pp. 103552, 2022.

[22] C. Xu, H. Wu, H. Liu, W. Gu, Y. Li, D. Cao, "Blockchain-oriented privacy protection of sensitive data in the internet of vehicles," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 2, pp. 1057-1067, 2022.

[23] W. Xu, H. Zhou, N. Cheng, F. Lyu, W. Shi, J. Chen, X. Shen, "Internet of vehicles in big data era," *IEEE/CAA Journal of Automatica Sinica*, vol. 5, no. 1, pp. 19-35, 2017.

[24] F. Yang, S. Wang, J. Li, Z. Liu, Q. Sun, "An overview of internet of vehicles," *China communications*, vol. 11, no. 10, pp. 1-15, 2014.

[25] M. Yang, I. Tjuawinata, K. Y. Lam, J. Zhao, L. Sun, "Secure hot path crowdsourcing with local differential privacy under fog computing architecture," *IEEE Transactions on Services Computing*, vol. 15, pp. 4, pp. 2188-2201, 2020.

[26] M. Yang, I. Tjuawinata, K. Y. Lam, T. Zhu, J. Zhao, "Differentially Private Distributed Frequency Estimation," *IEEE Transactions on Dependable and Secure Computing*, 2022.

[27] T. Ye, R. Kannan, V. K. Prasanna, "FPGA Acceleration of Fully Homomorphic Encryption over the Torus," in *2022 IEEE High Performance Extreme Computing Conference (HPEC). IEEE*, pp. 1-7, 2022.

[28] W. Yuan, H. Gao, "An Efficient BGV-type Encryption Scheme for IoT Systems," *Applied Sciences*, vol. 10, no. 17, pp. 5732, 2020.

Biography

Junting Zhang biography. Junting Zhang is with School of Automobile, Henan College of transportation. Research interests are Information security, Computing networks, Internet of vehicles security.

A Novel Differential Privacy Protection Model Based on Spectral Clustering Algorithm

Yudi Zhang

(Corresponding author: Yudi Zhang)

School of Electronic and Electrical Engineering, Zhengzhou University of Science and Technology
Zhengzhou 457600, China
Email: ljnan127@163.com

(Received Nov. 26, 2022; Revised and Accepted June 16, 2023; First Online June 25, 2023)

The Special Issue on Computational Intelligence Networks for Privacy and Security in Evolving Internet of Multimedia Things
Special Editor: Prof. Shoulin Yin (Harbin Institute of Technology)

Abstract

In recent years, with the vigorous development of the Internet and information technology, massive data can provide researchers with many practical information resources. Mining and analysis for these massive data can obtain precious information, among which cluster analysis is one of the effective means. Still, there is also the risk of privacy disclosure in the clustering process. However, there is also the problem of low efficiency of data use. This paper proposes a novel differential privacy protection model based on a spectral clustering algorithm to improve data availability and protect data privacy. Firstly, a spectral clustering algorithm is used to cluster data. Then, the cumulative distribution function is used to generate random noise satisfying the Laplace distribution. The noise is added to the function of sample similarity calculated by the spectral clustering algorithm, which interferes with the weight value between sample individuals and realizes information hiding between sample individuals. Finally, we evaluate the new approach's performance, data availability, and privacy performance on real data sets. The experimental results show that the privacy protection method in this paper can not only implement differential privacy protection but also significantly improve the efficiency of differential privacy data release.

Keywords: Cumulative Distribution Function; Data Security; Differential Privacy Protection; Spectral Clustering

1 Introduction

With the continuous development of Internet technology, people's clothes, food, housing and transportation are gradually digitized. But at the same time, the privacy leakage problem brought by big data has seriously affected people's life and work, "big data kill mature", "spam text message" and other phenomena are common [6, 28]. In real life, whether to realize "vigorous development of data" or "ensure data security" has become a serious problem in the development course of digital economy. How to protect privacy security under the background of big data is the focus of social attention and also an important research direction in the current academic circle.

At present, researchers have done a lot of work on privacy security protection. From the existing privacy protection technology: k-anonymity [13] and its extended protection model technologies have been widely used. This method conceals one data record by storing at least k records to achieve the purpose of privacy protection. However, if the attacker has the specific background knowledge, it may not be able to resist the consistent attack. In order to overcome this shortcoming, researchers keep trying to make improvements and emerge privacy protection technologies such as l-diversity [3], t-adjacent [19], (a, k)-anonymity [26], generalization and randomization [21] etc.

Nowadays, more and more applications of cluster analysis are applied in privacy protection. And clustering, as one of the main technologies of data mining and machine learning, has been studied by most scholars. The privacy protection techniques commonly used in cluster analysis include numerical perturbation, numerical rotation, numerical anonymity, etc. Hong *et al.* [9] proposed a new spatial data transformation method (Rotation-based Transformation, RT). The basis of this method was to hide information based on geometric rotation changes, and to ensure that the properties before and after rotation were still valid. Its disadvantage was that it could only transform low-dimensional data. When the dimension was high, the real information of the data would be lost, and the calculation amount would be large. Moreover, it was difficult to avoid the privacy leakage caused by consistency attack. Mukherjee *et al.* [18] proposed a new data perturbation method using Fourier trans-

form. The advantage of this method was that it could hide sensitive information while maintaining the validity of data values, and ensure the high accuracy of distance in Euclidean centralized and distributed scenarios. The current research on the combination of differential privacy technology on the basis of clustering is not mature enough. This idea was first proposed by Yuan *et al.*, [29] which combined differential privacy and k-means algorithm and used the administrator's identity to introduce noise into the query response to maintain the privacy of a single database entry. Subsequently, in 2018, Zhang *et al.* [31] further analyzed and improved the k-means algorithm based on differential privacy and proposed an algorithm that could calculate the sensitivity of query function and query sequence. Ge *et al.* [7] proposed IDP ε-means method under ε-difference privacy protection. This method could deal with the attack where the attacker had any background knowledge, and improved the availability of data clustering. However, this method could not solve the privacy leakage security problem in distributed environment. Therefore, Luo *et al.* [15] put forward the k-means algorithm satisfying ε-difference privacy in the distributed environment, and solved the problem that the traditional privacy protection model could not cope with the attack of arbitrary background knowledge in the distributed environment. Al-mamory *et al.* [2] proposed the DP-DBScan algorithm satisfying ε-difference privacy protection, which was developed in response to the privacy leakage problem existing in the traditional DBScan clustering algorithm. The experimental results showed that compared with the traditional DBScan clustering algorithm, the DP-DBScan algorithm with Laplacian noise could maintain the data validity and realize the privacy protection. Binjubeir *et al.* [4] adopted the anonymization technology based on clustering and used the differential privacy protection model to protect published data. This method realized anonymization through clustering, and added random noise to the anonymized differentiated data to disturb the real value of the data so as to achieve privacy protection and improve data availability. At present, there are few researches on the combination of clustering methods and differential privacy. This paper mainly focuses on the spectral clustering algorithm and carries out the research on spectral clustering algorithm based on differential privacy protection.

In order to solve the privacy leakage problem of clustering algorithm, this paper uses spectral clustering algorithm to cluster all kinds of private data together. In order to prevent such privacy data leakage, the Laplacian random noise of differential privacy is added to the weight calculation of similarity function to achieve privacy protection.

The organizational structure of this paper is as follows. In section 2, the related works are given. Proposed differential privacy protection model is shown in section 3. Experimental analysis is displayed in section 4. There is a conclusion in section 5.

2 Related Works

The main problems of traditional anonymous method are as follows: (1) it cannot resist background attacks, such as Netflix privacy leakage incident; (2) It is difficult to integrate with deep learning. This kind of method modifies the records in the original data set to achieve generalization or suppression of user sensitive attributes, while deep learning requires direct extraction and training of data features, which makes it difficult to combine the two theoretically [27]. In the existing studies, when the differential privacy technology is applied to deep neural networks, the noise addition location includes input, member parameters, such as gradient and weight parameters, objective function and output. Differential privacy technology provides reliable privacy protection, ensuring that even if an adversary has all the information except the target object, it cannot infer whether a particular record is contained in the database. For example, Wei *et al.* [25] proposed a DP-SGD algorithm to compute the gradient of a random subset of a training sample, trim each gradient according to the L2-norm, and add noise to the cumulative gradient of each batch. Liu *et al.* [14] added global gradient noise to generate adversarial network gradient, and used some public data sets to calculate the gradient mean as the optimal initial gradient clipping threshold to participate in deep differential privacy training. Liu *et al.* [12] used the non-uniform Gaussian mechanism to calculate noise and added heterogeneous noise into the batch cumulative gradient to effectively improve the robustness of the algorithm. Rathore *et al.* [20] developed a data encryption method for Internet of Vehicles communication and verification using distinct symmetric encryption for vehicle communication. Lyu *et al.* [16] highlighted the intuitions, key techniques, and fundamental assumptions adopted by various attacks and defenses. Song *et al.* [22] designed an efficient privacy-preserving data aggregation mechanism for federated learning to resist the reverse attack. Ma *et al.* [17] proposed an improved version of the MK-CKKS multi-key homomorphic encryption protocol to design a novel privacy-preserving federated learning scheme. Hamian *et al.* [8] introduced a blockchain-based user re-enrollment for biometric-based authentication schemes using a secure multi-party sum protocol. Blockchain technology had dismissed the need for a trusted server. Adil *et al.* [1] presented a robust channel categorization scheme to fix data privacy and preservation problems in an Industrial Healthcare Internet of Things (IHC-IoT) network. The proposed model categorized the transmission bandwidth into four independent channels for each device by defining triggering rules with respect to time for reception and transmission of data. These studies can well resist member inference attacks, but the cost is to reduce the availability of data. How to improve the training accuracy under the same privacy budget is a major difficulty in these method.

Differential privacy can usually be used in non-interactive scenarios [11], which can provide a strong pri-

vacy guarantee. No matter whether the data set contains records of the individual information, the response results returned for any query operation are similar. That is, inserting or deleting a record from a dataset has no effect on the output of the query. The basic definitions of differential privacy and spectral clustering are given below.

2.1 Spectral Clustering Algorithm

At present, spectral clustering (SC) algorithm [23] has been widely applied and researched, and the most commonly applied fields include machine learning, big data mining, image segmentation, text mining, etc. The process of SC is simple, and it is more applicable than the traditional k-means and expectation maximization (EM) algorithm. SC can achieve the best clustering effect in any data sample space. The main idea of SC is the segmentation technique based on graph theory. SC treats sample data as one vertex in undirected weighted graph. Then the similarity function is used to calculate the value between each vertex, and the weight value represents the similarity between each vertex. The data is segmented and clustered by the segmentation criterion of the graph.

The similarity function of general spectral clustering algorithm adopts cosine function and Gaussian function, which are specifically defined as follows:

$$sim(X,Y) = cos\theta = \frac{X \cdot Y}{||X|| \cdot ||Y||}. \quad (1)$$

$$W_{ij} = exp(-\frac{d(s_i,s_j)}{2\sigma^2}). \quad (2)$$

The main criteria of graph segmentation algorithm are as follows:

1) Graph segmentation minimum segmentation method criteria:

$$Cut(A,B) = \sum_{u \in A, v \in B} w(u,v)$$

2) Normalized segmentation criteria:

$$Normalized_Cut(A,B) = \frac{Cut(A,B)}{sum(A,V)} + \frac{Cut(A,B)}{sum(B,V)}$$

3) Min-Max segmentation criterion:

$$Mcut(A,B) = \frac{Cut(A,B)}{sum(A,A)} + \frac{Cut(A,B)}{sum(B,B)}$$

4) Proportional segmentation criteria:

$$Rcut(A,B) = \frac{Cut(A,B)}{min(|A|,|B|)}$$

The main algorithm flow of spectral clustering algorithm is shown in **Algorithm 1**.

Algorithm 1 SC algorithm

1: **Input:** Data point set n, clustering number k.
2: **Output:** k cluster partition.
3: Calculate the similarity matrix by the distance formula of Gaussian kernel function;
4: Construct the adjacency matrix N and degree matrix G using the similar matrix;
5: Laplacian matrix $L = G^{1/2}NG^{1/2}$ is obtained from the obtained adjacency matrix and degree matrix;
6: After obtaining the Laplacian matrix, select the eigenvectors corresponding to the first k maximum eigenvalues;
7: Standardize the feature vectors, and then map the sample data points to one or more defined dimensionality reduction Spaces;
8: Based on the new data point space, each row of the feature matrix is regarded as a sample point and aggregated into class k by k-means.

2.2 Differential Privacy

Differential privacy protection model has a strict mathematical theoretical basis, and the basic idea of this model is to add noise to data to achieve the purpose of privacy protection [10]. This protection method does not need to care about the attacker's computing power and any background knowledge. Even if an attacker has all the data records except one, it can guarantee that sensitive information about that record will not be disclosed. This mechanism can protect individual sensitive information in sample data without changing data distribution. The specific definition of differential privacy is as follows:

Definition 1. *Assume that data sets D and D' are adjacent data sets and that the two data sets are identical or differ by at most one data record. Given a random algorithm S, $Range(S)$ is the value range of algorithm S, R_M is the output result on the data set, $Pr[X]$ is the disclosure risk of event X, then algorithm S satisfies the definition of ε-difference privacy protection model:*

$$Pr[S(D) = R_M] \leq exp(\varepsilon) Pr[S(D') = R_M]. \quad (3)$$

The value of privacy disclosure risk is controlled by the random algorithm S, and the security degree of privacy protection is controlled by limiting the size of ε. The smaller ε is, the greater the random noise is introduced and the higher the privacy protection security is. The larger ε is, the smaller random noise is introduced and the lower the security of privacy protection.

Definition 2. *The sensitivity of the function $F : D \to R^d$ is defined as follows:*

$$\Delta F = \max_{D,D'} ||F(D0 - F(D')||_1. \quad (4)$$

Where $||\cdot||_1$ is the first-order norm. F is the query function. d is the attribute dimension of recorded data. D and D' are data sets that differ by at most one data record. R is the space of real numbers.

Definition 1 shows that the selection of random function has nothing to do with the background knowledge of the attacker, so the addition or deletion of any record will not affect the output of the query result. This definition meets the requirement of differential privacy on privacy disclosure risk theoretically, but the concrete realization depends on adding noise mechanism.

3 Proposed Differential Privacy Protection Model

3.1 Comparison Between Spectral Clustering and Other Cluster Methods

According to different classification criteria, there are many clustering methods. Classical clustering methods include K-means algorithm and DBSCAN algorithm based on density division. K-means algorithm has the characteristics of fast speed and simple algorithm implementation. However, the traditional k-means algorithm for differential privacy protection is sensitive to the selection of initial point, and the selection of clustering number k value is blind and arbitrary. In other words, different initial points and the selection of k value can lead to different clustering results. For example, Zhang *et al.* [30] proposed an improved differential privacy K-means algorithm, which improved the convergence and availability of clustering. However, because the K value of k-means needs to be specified artificially, it has its own limitations, which brings uncertainty to the subsequent privacy protection. Compared with K-means, DBSCAN algorithm can find clusters of any shape without specifying the number of clusters formed in advance. At the same time, the algorithm can identify noise points well and has good robustness to outliers. However, when the dimension of the data set is large, it cannot reflect the density of data change well. For example, although the MDAV clustering method described in literature [5] had been greatly improved in the clustering effect and operation mode, it still had some problems such as high complexity and inapplicability to non-numerical attributes. Considering the advantages and limitations of the classical algorithm, this paper focuses on improving the shortcomings of the classical algorithm, and uses spectral clustering to realize the micro-aggregation step. First of all, spectral clustering does not need to set the number of clusters in advance, which makes the clustering results more reasonable and normative. Moreover, it adds the adjacency relation to the center of mass of the cluster, that is, the sample sets between neighbors are more correlated than those between non-neighbors, resulting in higher homogeneity within the cluster. Moreover, the model has self-stability, can adapt the weight, and can learn in real time, which greatly facilitates the search for the optimal solution. At the same time, it has strong anti-noise ability, which makes the clustering sensitivity of the final obtained low.

3.2 MDAV Data Protection Method

The original data set can not be protected by clustering operation only. In order to prevent sensitive information from being leaked, it is necessary to implement differential privacy protection for data sets. However, the realization of differential privacy requires the addition of large noise to the data set, which results in large data distortion. The Algorithm 2 of MDAV data protection method is as follows.

Algorithm 2 MDAV Data Protection

Input: data set D, degree of anonymity k.
Output: D'.
while $|D| \geq 3k$ **do**
  Calculate the mean r_0 of all records in D.
  With r_0 as the center, find the record r farthest from the center, and then find the record s farthest from r.
  With r as the center, $k-1$ records closest to r are selected to form a cluster.
  With s as the center, $k-1$ records closest to s are selected to form another cluster.
  Periodically refresh the *observations storage*
end while
if $|D| \geq 2k$ **then**
  Recalculate the data center according to Step 2 and repeat the preceding process until the number of remaining records is less than $2k$.
end if
Group the remaining records together.
Noise obeying Y $Lap(\Delta f/\varepsilon)$ is added to each of the above clusters.
return D'.

To some extent, this algorithm still uses the idea of first processing the original data and then adding noise. In terms of clustering mode, K-means makes further improvement on the selection of initial points, and also reduces the noise required for differential privacy to a certain extent, but it still cannot avoid the defects of ordinary clustering mode (initial point selection). The processing results of data sets with different data structures will be quite different, so the clustering effect cannot be guaranteed. Therefore, the algorithm integrating machine learning with differential privacy can protect data privacy, improve data utility, and reduce the influence of human factors on clustering effect.

3.3 Differential Privacy Based on SC

In order to solve the limitations of the above algorithms and improve the data utility, a new DPSC (Differential Privacy Based on SC) algorithm is proposed. The specific approach is to first carry out micro-aggregation operation on the original data set, train an SC model using the machine learning training mode, and then map the original data set into the corresponding clustering. Adding noise

to each divided cluster is far less than the total amount needed to add it to each record. Moreover, SC clustering has the advantage of being insensitive to noise, that is, the data set will be less affected by noise. Finally, the noise satisfying differential privacy is added to the processed clustering, which makes the data utility of the data set to be published significantly improved. **Algorithm 3** shows the specific process of differential privacy protection.

Algorithm 3 DPSC process

Input: Data set $D = x_1, x_2, \cdots, x_n$ with n records, learning rate $\eta \in (0, 1)$.

Output: Data set $D(\varepsilon)$ satisfying ε-differential privacy.

Initializing weight $w_{ij} \in [0, 1]$, w_{ij} is a different random value and determines the neighborhood size δ.

Sampling, taking n dimensional vector x from the data set space with a certain probability to represent the activation mode applied to the grid.

while —D—¿0 **do**

Calculate space distance d_j; d_j is the distance between all input node x_i at time t and output node, using Euclidean distance $d_j = \sum_{i=1}^{n}(x_i(t) - w_{ij}(t))^2$.

Select the winning neuron $i(x)$, so that it satisfies $i(x) = min_j(d_j)$.

Adjust the connection weight vector between the output node and its neighborhood node, $w_{ij}(t + 1) = w_{ij}(t) + \eta(t)h_{j,i(x)}(x(t) - w_{ij}(t))$. $h_{j,i}(x)(t)$ is the domain function around the winning neuron.

end while

The trained model φ is obtained.

Apply data set D to φ and map to m clusters $C_1, C_2, \cdots, C_m$, and the center of mass of each cluster is denoted as a_0^i.

For $C_1, C_2, \cdots, C_m$ adds Laplacian noise.

The probability density function satisfies the ε-difference privacy definition.

return $D(\varepsilon)$.

The DPSC model is based on neural network mapping to obtain several clusters of different sizes. The sensitivities vary for the centroid of different clusters. Since the sensitivity depends on the base of clustering, as long as the sensitivity Δf_i of the centroid is calculated, the difference privacy can be satisfied by adding Laplasian noise with mean 0 and scale $\Delta f_i/\varepsilon$. According to the differential privacy parallel combination theorem, adding noise to each cluster makes it satisfy the differential privacy, then the whole data set can satisfy the differential privacy definition. The proof is shown below.

Suppose data set D is mapped by DPSC model to obtain several clusters of similar scale, then $D = C_1 \cup C_2 \cup C_3 \cup \cdots \cup C_n$, $D' = C_1' \cup C_2' \cup C_3' \cup \cdots \cup C_n'$. According to Equations (3) and (4):

$$P(M(C_1) \in S) = \frac{\varepsilon_1}{\Delta f_1} exp(-\frac{\varepsilon_1}{\Delta f_1})|f(C_1)|. \quad (5)$$

$$P(M(C_1') \in S) = \frac{\varepsilon_1}{\Delta f_1} exp(-\frac{\varepsilon_1}{\Delta f_1})|f(C_1')|. \quad (6)$$

It can be obtained by dividing Equation (5) by Equation (6).

$$\frac{P(M(C_1) \in S)}{P(M(C_1') \in S)} = exp(\frac{\varepsilon_1}{\Delta f_1} \times A) \leq exp(\varepsilon_1) + \delta. \quad (7)$$

Here, $A = |f(C_1) - f(C_1')|$. It only needs $|f(C_1) - f(C_1')| \leq \underset{C_1, C_1'}{max} |f(C_1) - f(C_1')| = \Delta f_1$, let $\Delta f_1 = |f(C_1) - f(C_1')|$, it can satisfy ε_1, δ-differential privacy.

3.4 Algorithm Complexity Analysis

The time complexity of the algorithm reflects the computational workload required to implement the algorithm. The complexity can be analyzed according to the above algorithm. SC is a typical hierarchical clustering algorithm, and DPSC algorithm is its differential privacy implementation. Assume that there are n records in the data set, while loop is to construct m clusters, the number of loops does not exceed n/m, and this operation is completed in $O(n)$ time. The closest distance of record traversal should be selected for each cluster within the cycle. The number of iterations within the cluster is t, and the time complexity of SC clustering algorithm is $m \times t \times O(n)$. According to the above analysis, the time complexity of DPSC algorithm is $O(n^2)$.

4 Experimental Analysis

Data sets with different attributes and sizes in UCI(http://archive.ics.uci.edu/ml) database are adopted as shown in Table 1.

4.1 Experimental Evaluation Criteria

The quality of data mining for privacy protection depends on the degree of privacy information protection and the accuracy of mining results. The privacy protection level of clustering is evaluated by ε. ε is negatively correlated with the effect of privacy protection, that is, the larger ε is, the smaller the noise added, and the worse the effect of privacy protection is.

The effectiveness of clustering is evaluated by Calinski-Harbasez index (CH) [24]. Suppose CN is the number of subsets that a hard partition clustering algorithm divides the data set into different parts, then $D = (x_1, x_2, \cdots, x_n) = (C_1, C_2, \cdots, C_{CN})$. Where $1 \leq i \leq CN$. Subset C_i is a subcluster of data set D. N_i is the number of objects in subcluster C_i. c represents the center point of dataset D. c_i represents the center point of subcluster C_i. $d(x, y)$ is the distance between x and y.

The expression formula of CH clustering effectiveness evaluation index is as follows.

$$CH(CN) = \frac{\frac{1}{CN-1} \times \sum_{i=1}^{CN} N_i \times d^2(c_i, c)}{\frac{1}{n-CN} \times \sum_{i=1}^{CN} \sum_{x \in C_i} \times d^2(x, c)} \quad (8)$$

Table 1: Data set

Set	Alias	Type	Attribute	record number
Wine	D1	Real	13	178
Haberman	D2	Real	4	306
Waveform Database	D3	Real	40	50000
MAGIC	D4	Real	11	19020

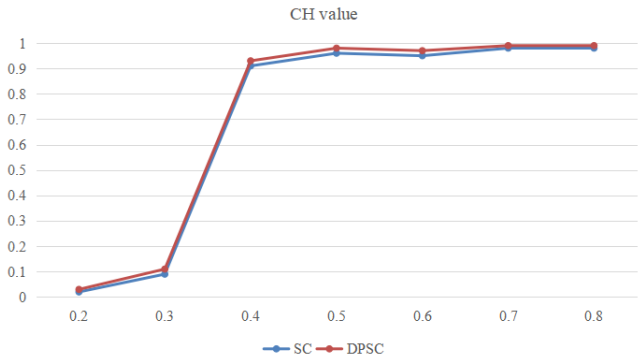


Figure 1: CH value on D1

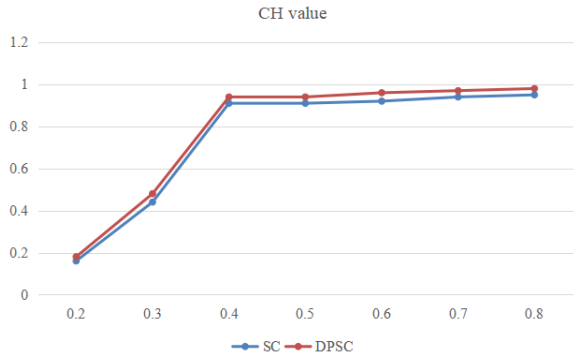


Figure 2: CH value on D2

As can be seen from the above formula, CH index measures the tightness of a cluster by calculating the sum of the squares of the distance between each point in the class and the cluster center, and measures the separation of the data set by calculating the sum of the squares of the distance between each center point of the cluster and the center point of the data set. CH is the ratio of the two values. Therefore, the larger CH value denotes the more discrete between the clusters, and better clustering efficiency.

4.2 Experimental Results and Analysis

Due to the randomness of adding noise, SC clustering algorithm is invoked for multiple clustering analysis on each data set. It takes the average value of CH and plots the CH ratios of the two algorithms (SC and DPSC) on data sets D1, D2, D3 and D4, respectively. The closer the CH ratio is to 1, the clustering effectiveness of the two clustering algorithms is closer. The experimental results are shown in Figures 1 $\sim$ 4.

Experimental results show that DPSC clustering algorithm has the following characteristics:

1) By comparing Figures 1,2,3,4, it can be seen that DPSC clustering algorithm for differential privacy protection satisfies ε-differential privacy protection, eliminates hidden dangers of privacy disclosure in the clustering process under a strictly defined attack model, and can effectively protect personal privacy.

2) As shown in Figures 1,2,3,4, DPSC clustering algorithm for differential privacy protection can achieve

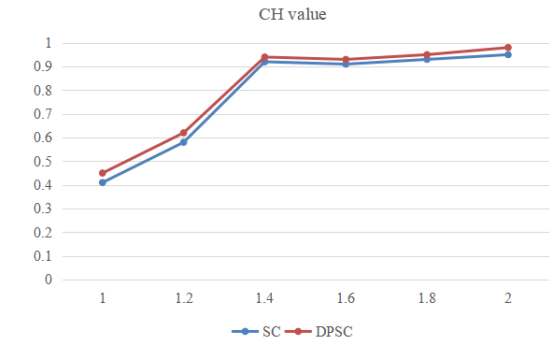


Figure 3: CH value on D3

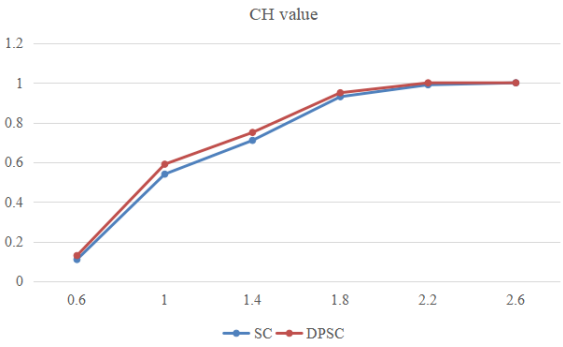


Figure 4: CH value on D4

better privacy protection effect by adding a small amount of noise, and also ensure the clustering effectiveness similar to the traditional SC clustering algorithm. The privacy protection level depends on the value of ε. It can control the privacy protection level based on the value of ε. The smaller ε denotes the higher privacy protection level.

3) By comparing Figures 1,2,3,4, it can be seen that, under the same privacy protection level, the DPSC clustering algorithm for differential privacy protection has a higher clustering effectiveness for small data sets than for large data sets, and a higher clustering effectiveness for low-dimensional data sets than for high-dimensional data sets.

5 Conclusions

In order to balance the utility of differential privacy data and privacy protection, a differential privacy algorithm based on spectral clustering is proposed. Firstly, the advantages and disadvantages of differential privacy and SC clustering are analyzed, and then the theoretical analysis results show that DPSC algorithm is better than similar algorithms. Finally, experimental tests are carried out on real data sets, and it is proved that DPSC can satisfy differential privacy and reduce data information loss at the same time, that is, under the premise of privacy protection, greatly improve the availability of data release. In the future work, the author plans to conduct in-depth exploration of algorithms for large complex data sets, and further consider the utility and privacy protection of data release of mixed data sets on the basis of machine learning.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] M. Adil, M. Attique, M. M. Jadoon, J. Ali, A. Farouk, H. Song, "HOPCTP: a robust channel categorization data preservation scheme for industrial healthcare internet of things," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 10, pp. 7151-7161, 2022.

[2] S. O. Al-mamory, I. S. Kamil, "A New Density Based Sampling to Enhance Dbscan Clustering Algorithm," *Malaysian Journal of Computer Science*, vol. 32, no. 4, pp. 315-327, 2019.

[3] J. Andrew, J. Karthikeyan, "Privacy-preserving big data publication:(K,L)-anonymity," in *Intelligence in Big Data Technologies Beyond the Hype: Proceedings of ICBDCC 2019. Springer Singapore*, pp. 77-88, 2021.

[4] M. Binjubeir, A. Ahmed, M. Ismail, A. Sadiq, M. Khan, "Comprehensive survey on big data privacy protection," *IEEE Access*, vol. 8, pp. 20067-20079, 2019.

[5] J. Deng, J. Guo, Y. Wang, "A Novel K-medoids clustering recommendation algorithm based on probability distribution for collaborative filtering," *Knowledge-Based Systems*, vol. 175, pp. 96-106, 2019.

[6] W. Fang, X. Z. Wen, Y. Zheng, M. Zhou, "A survey of big data security and privacy preserving," *IETE Technical Review*, vol. 34, no. 5, pp. 544-560, 2017.

[7] L. Ge, Y. Hu, H. Wang, Z. He, H. Meng, X. Tang, L. Wu, "IDP-OPTICS: improvement of differential privacy algorithm in data histogram publishing based on density clustering," in *Intelligent Computing Theories and Application: 15th International Conference, ICIC 2019, Nanchang, China, August 3-6, 2019, Proceedings, Part II 15. Springer International Publishing*, pp. 770-781, 2019.

[8] N. Hamian, M. Bayat, M. R. Alaghband, Z. Hatefi, S. M. Pournaghi, "Blockchain-based User Re-enrollment for Biometric Authentication Systems," *IJ of Electronics and Information Engineering*, vol. 14, no. 1, pp. 18-38, 2022.

[9] D. Hong, A. Mohaisen, "Augmented Rotation-Based Transformation for Privacy-Preserving Data Clustering," *Etri Journal*, vol. 32, no. 3, pp. 351-361, 2010.

[10] J. W. Kim, K. Edemacu, J. S. Kim, Y. D. Chung, B. Jang, "A survey of differential privacy-based techniques and their applicability to location-based services," *Computers & Security*, vol. 111, pp. 102464, 2021.

[11] C. Lan, H. Li, S. Yin, L. Teng, "A New Security Cloud Storage Data Encryption Scheme Based on Identity Proxy Re-encryption," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 804-810, 2017.

[12] J. Liu, J. Lou, L. Xiong, X. Meng, "Projected federated averaging with heterogeneous differential privacy," *Proceedings of the VLDB Endowment*, vol. 15, no. 4, pp. 828-840, 2021.

[13] J. Liu, S. Yin, H. Li, L. Teng, "A Density-based Clustering Method for K-anonymity Privacy Protection," *J. Inf. Hiding Multim. Signal Process*, vol. 8, no. 1, pp. 12-18, 2017.

[14] M. Liu, Z. Zhuang, Y. Lei, C. Liao, "A Communication-Efficient Distributed Gradient Clipping Algorithm for Training Deep Neural Networks," *Advances in Neural Information Processing Systems*, vol. 35, pp. 26204-26217, 2022.

[15] Y. Luo, Z. Wang, S. Zhang S, J. Liu, "Efficient-Secure k-means Clustering Guaranteeing Personalized Local Differential Privacy," in *Algorithms and Architectures for Parallel Processing: 22nd International Conference, ICA3PP 2022, Copenhagen, Denmark, October 10-12, 2022, Proceedings. Cham: Springer Nature Switzerland*, pp. 660-675, 2023.

[16] L. Lyu, H. Yu, X. Ma, C. Chen, L. Sun, J. Zhao, Q. Yang, P. S. Yu, "Privacy and Robustness in Federated Learning: Attacks and Defenses," *IEEE Transactions on Neural Networks and Learning Systems*, 2022. DOI: 10.1109/TNNLS.2022.3216981.

[17] J. Ma, S. A. Naas, S. Sigg, X. Lyu, "Privacy-preserving federated learning based on multi-key homomorphic encryption," *International Journal of Intelligent Systems*, vol. 37, no. 9, pp. 5880-5901, 2022.

[18] S. S. Nourazar, A. Nazari-Golshan, "A new modification to homotopy perturbation method combined with Fourier transform for solving nonlinear Cauchy reaction diffusion equation," *Indian Journal of Physics*, vol. 89, pp. 61-71, 2015.

[19] V. Puri, P. Kaur, S. Sachdeva, "(k,m,t)-anonymity: Enhanced privacy for transactional data," *Concurrency and Computation: Practice and Experience*, vol. 34, pp. 18, pp. e7020, 2022.

[20] M. S. Rathore, M. Poongodi, P. Saurabh, U. K. Lilhore, S. Bourouis, W. Alhakami, J. Osamor, M. Hamdi, "A novel trust-based security and privacy model for internet of vehicles using encryption and steganography," *Computers and Electrical Engineering*, vol. 102, pp. 108205, 2022.

[21] F. Song, T. Ma, Y. Tian, M. Al-Rodhaan, "A new method of privacy protection: random k-anonymous," *IEEE Access*, vol. 7, pp. 75434-75445, 2019.

[22] J. Song, W. Wang, T. R. Gadekallu, J. Cao, Y. Liu, "Eppda: An efficient privacy-preserving data aggregation federated learning scheme," *IEEE Transactions on Network Science and Engineering*, 2022. DOI: 10.1109/TNSE.2022.3153519.

[23] G. Sun, Y. Cong, J. Dong, Y. Liu, Z. Ding, H. Yu, "What and how: generalized lifelong spectral clustering via dual memory," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 44, no. 7, pp. 3895-3908, 2021.

[24] S. ɾukasik, P. A. Kowalski, M. Charytanowicz, P. Kulczycki, "Clustering using flower pollination algorithm and Calinski-Harabasz index," in *2016 IEEE congress on evolutionary computation (CEC). IEEE*, pp. 2724-2728, 2016.

[25] J. Wei, E. Bao, X. Xiao, Y. Yang, "DPIS: An Enhanced Mechanism for Differentially Private SGD with Importance Sampling," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (ACM CCS 2022)*, pp. 2885-2899, 2022.

[26] R. Wong, J. Li, A. Fu, K. Wang, "(α, k)-anonymity: an enhanced k-anonymity model for privacy preserving data publishing," in *Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining*, pp. 754-759, 2020.

[27] M. Yang, I. Tjuawinata, K. Y. Lam, "K-Means Clustering With Local d_x-Privacy for Privacy-Preserving Data Analysis," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2524-2537, 2022.

[28] M. M. Yang, I. Tjuawinata, K. Y. Lam, T. Zhu, "Differentially Private Distributed Frequency Estimation," *IEEE Transactions on Dependable and Secure Computing*, 2022. doi: 10.1109/TDSC.2022.3227654.

[29] L. Yuan, S. Zhang, G. Zhu, K. Alinani, "Privacy-preserving mechanism for mixed data clustering with local differential privacy," *Concurrency and Computation: Practice and Experience*, pp. e6503, 2021. https://doi.org/10.1002/cpe.6503.

[30] E. Zhang, H. Li, Y. Huang, S. Hong, L. Zhao, C. Ji, "Practical multi-party private collaborative k-means clustering," *Neurocomputing*, vol. 467, pp. 256-265, 2022.

[31] Y. Zhang, N. Liu, S. Wang, "A differential privacy protecting K-means clustering algorithm based on contour coefficients," *PloS One*, vol. 13, no. 11, pp. e0206832, 2018.

Biography

Yudi Zhang biography. Yudi Zhang is with School of Electronic and Electrical Engineering, Zhengzhou University of Science and Technology, Zhengzhou City, Henan Province, 450064, China. Research interests are data security and Information encryption processing.

FLADA: Federated Learning-based Association Domain Adaptive Scheme for English Data Privacy Protection

Xiaobin Guo

(Corresponding author: Xiaobin Guo)

Zhengzhou Railway Vocational and Technical College
56 Pengcheng Avenue, Zhengdong New District, Zhengzhou City, 450018 China
Email: publicgj@163.com

(Received Oct. 20, 2022; Revised and Accepted June 16, 2023; First Online June 25, 2023)

The Special Issue on Computational Intelligence Networks for Privacy and Security in Evolving Internet of Multimedia Things
Special Editor: Prof. Shoulin Yin (Harbin Institute of Technology)

Abstract

As internationalization becomes more and more intense, the security of English data is also paid more and more attention. Aiming at the problems of traditional data privacy protection algorithms, such as long execution time, high concealment rate, and poor adaptability, this paper proposes a federated learning-based association domain adaptive scheme for English data privacy protection. In traditional federated learning, these model parameters reveal sensitive information and rely on trusted third-party servers. The new association domain adaptive federal learning privacy protection scheme proposed in this paper can resist server attacks, user attacks, and joint attacks on servers. This new scheme comprises three protocols: key exchange, association domain adaptive, and disconnection processing. Experiments show that the privacy protection model proposed in this paper achieves the trade-off between privacy and practical accuracy with superior performance on data sets MNIST and SVHN.

Keywords: Association Domain Adaptive; Data Privacy Protection; Disconnection Processing; Federated Learning

1 Introduction

Deep learning technology is increasingly widely used in all walks of life. However, the model accuracy of deep learning is directly proportional to the quantity, and enterprises with a small amount of data may make wrong judgment results, resulting in the emergence of the mode of concentrated learning [11, 20].

The establishment of these laws and regulations in different degrees put forward new challenges to the centralized learning mode, making the data training back to the "data island" state. Each enterprise has local limitations and small amounts of data, so accurate model predictions cannot be obtained. In 2016, a new solution – federated learning (FL) [15] was proposed. With the advent of federated learning, cross-enterprise model training ensures model accuracy and data security. In federated learning, users train machine learning models locally based on their own private data, and then share model parameters with servers to improve model performance.

The federated learning process can be summarized as:

1) The server delivers the initialization model to all users of federated learning.
2) Each user trains a common model on local privacy data, and then sends model parameters to the server.
3) The server aggregates model parameters sent by all users, obtains a global parameter, and sends the global parameter to each user.
4) Repeat the first three processes until the model converges.

It not only ensures data security, but also collaboratively trains a more accurate global model. All users participating in federated learning are beneficiaries of the model [26].

Although federated learning can solve the problem of privacy data exposure in traditional centralized learning mode, it still faces new privacy theft attacks such as member inference and attribute inference. A lot of research has been done on the privacy protection of federal learning. Aiming at the shortcomings of existing studies, this paper proposes a new association domain adaptive federal learning privacy protection scheme, which can effectively prevent users and servers from inferring privacy information through model parameters. Experimental results show

that the proposed scheme can achieve an effective balance between privacy protection and model performance.

In this paper, we organize this paper as follows. Related works are introduced in Section 2. We detailed design the proposed scheme in Section 3. Rich experiments are shown in Section 4. There is a conclusion in Section 5.

2 Related Works

2.1 Federated Learning

In the federated learning model, multiple users and servers can achieve model training only by sharing local parameters and aggregate parameters without collecting the original privacy data of users. However, existing studies [2, 21] show that attackers can indirectly obtain sensitive information based on shared model parameters. The sharing model is updated based on this private data, and its patterns are encoded into the model parameters. If the corresponding decoder can be constructed, the sensitive information in the user data can be inferred according to the model parameters of the user, and even the privacy data of the user can be deduced backwards.

Reference [16] had made a comprehensive analysis and summary of the privacy issues faced by federal learning. The attack types of federation learning mainly included member inference attack and attribute inference attack. Member inference attacks were based on a given record could determine whether in the training data. Attributive reasoning attacks were used to obtain data attribute information such as gender distribution, age distribution, income distribution and prevalence rate. Chamikara *et al.* [5] proposed a federated deep learning attack method for servers. For a specific user, a generative adversarial network (GAN) [14] was trained based on the updated parameters and the shared parameters of the server during each iteration, and the specific privacy data of the user was recovered. Jebreel *et al.* [12] proposed a federated learning attack. The server could train a binary classifier to judge data attributes by using the updated gradient value as input according to the update model of each stage. Wang *et al.* [23] proposed an asynchronous federated learning system based on permissioned blockchains, using permissioned blockchains as the federated learning server, which was composed of a main-blockchain and multiple sub-blockchains, with each sub-blockchain responsible for partial model parameter updates and the main-blockchain responsible for global model parameter updates. Tang *et al.* [22] proposed a network intrusion detection method based on federated learning. This method allowed multiple ISPs or other institutions to conduct joint deep learning training on the premise of retaining local data. It not only improved the detection accuracy of the model but also protected privacy in network traffic. In reference [7], to ensure the confidentiality and integrity of the information stored, encryption and auditing procedures were frequently used. Access control mechanisms were mostly used during the data sharing stage to regulate the objects that had access to the data. Huang *et al.* [10] proposed a 5G-V2X-oriented asynchronous federated learning privacy-preserving computing model. They used an adaptive differential privacy mechanism to reduce noise while protecting data privacy.

At present, most researchers defend against attacks on federated learning model from the perspective of parameter security aggregation. In federated learning parameter security aggregation, each user trains a model on local private data and sends the model parameters to the server in a secure manner [1]. The server is only responsible for aggregation. Among them, the methods of parameter security aggregation mainly include homomorphic encryption and secure multi-party computation.

Homomorphic encryption is a way to process data without accessing the data itself. Joye *et al.* [13] proposed to use two homomorphic encryption algorithms, LWE and Paillier, to hide model parameters when uploading parameters. After the server updates parameters, users decrypt model parameters for iterative training. Based on the Paillier method, Kwabena *et al.* [17] conducted a homomorphic encryption and aggregation for the forward and backpropagation parameters of each layer of the neural network. Ma *et al.* [18] proposed a multi-party deep learning privacy protection scheme based on the ElGamal method. Babenko *et al.* [4] proposed a homomorphic encryption scheme based on the Chinese residual theorem. Although homomorphic encryption could realize the safe aggregation of federated learning, it was inefficient and had heavy computation. Also, when one user collaborated with the server, it was easy for the server to obtain model parameters for all users.

2.2 Network Data Privacy Protection Based on Density Clustering

According to the characteristics of the network in the big data environment, the arbitrary shape of the cluster is generated. Finally, for the successfully generated clusters, it calculates the number of real nodes that should generate network privacy data in each cluster [6]. By adding edge and other technical means, it completes the protection of network data information privacy. The process is described as follows:

Definition 1. *Network privacy data quantifies the amount of information loss. It is assumed that Clt is a cluster in the network, and the quasi-identifier is expressed as:*

$$Q = (n_1, n_2, \cdots, n_s, c_1, c_2, \cdots, c_t). \tag{1}$$

Then, the network privacy data information loss generated by the generalization quasi identifier is:

$$QL(Clt) = |Clt| \times [\sum_{i=1}^{s} \frac{Range(n_i)}{sub(c)}]. \tag{2}$$

Where, $|Clt|$ is the number of nodes in network clusters. n_i indicates the node degree of the network privacy

data cluster. If the number of generated clusters is m, the total information loss of network privacy data is:

$$TQL(G) = \sum_{i=1}^{m}(QL(Clk)). \tag{3}$$

Definition 2. *The amount of information lost in network privacy data structure. Assume that the network $G = (V, E)$, $V = v_1, v_2, \cdots, v_n$ in the big data environment. The node set of a cluster Clk in the network is $V = v_1, v_2, \cdots, v_n$, then the degree of node v_i in the network cluster is $k(v_i)$, and the expression formula of the maximum number of edges that can be formed by other network nodes connected with node v_i is:*

$$T(v_i) = k(v_i) \times (k(v_i) - 1)/2. \tag{4}$$

Where, k represents the privacy parameter of network data. In the big data environment, the actual number of edges formed by other network nodes connected to network node v_i is $E(v_i)$, then the network aggregation coefficient of network node v_i is calculated as:

$$C(v_i) = E(v_i)/T(v_i). \tag{5}$$

Therefore, the sum of aggregation coefficients of network G in the big data environment is:

$$FQL = \sum_{i=1}^{n} C(v_i). \tag{6}$$

According to Equation (6), the aggregation coefficient of network cluster Clt is calculated as:

$$EQL = \sum_{i=1}^{m}(\sum_{i=1}^{|CL|} C(v_i)). \tag{7}$$

Where, $|CL|$ represents the limiting threshold of network privacy data. The formula for calculating the total structure information loss of network privacy data is as follows:

$$NTQL = FQT - EQL. \tag{8}$$

Assuming that the total number of real nodes in the generating network is N and the number of generation clusters is m, then the number of real network users generated in each cluster is N_i.

$$N_i = (\frac{n_i}{n_1 + n_2 + \cdots + n_m}) \times N. \tag{9}$$

Where, n_i represents the number of nodes in the $i-th$ cluster of the network, and $1 \leq i \leq m$. Finally, on the premise of not changing the connection of other network nodes, the network node with the least degree is selected to connect with the newly generated real network node respectively. In this way, network data privacy protection can be realized in the big data environment.

3 Scheme Design

Aiming at the problems existing in the federal learning privacy protection scheme, this paper proposes a new federal learning association domain adaptive (FLADA) privacy protection scheme. The scheme mainly includes three protocols: key exchange protocol, association domain adaptive (ADA) protocol and dropped-line processing protocol.

In the key exchange protocol, a common key value is negotiated between two users. The Diffie-Hellman key negotiation [25] method is used to implement the key exchange protocol. Based on the difficulty of the discrete logarithm, this method can ensure that other users cannot obtain the key value.

In the ADA protocol, the double masking method [9] has the problem of relying on the trusted server, which can obtain the aggregated model parameters. This paper proposes a new ADA scheme to ensure the safety of users and aggregated model parameters. At the same time, if a user uploads model parameters after the server executes the off-line processing protocol, the model parameters of the delayed user will not be exposed.

In the drop-out processing protocol, each user shares the private key in the key exchange protocol with other users based on Shamir key sharing [24] technology. Once a user drops out, the server can perform secret recovery to eliminate the hidden value of the dropped user.

Security assumption:

1) Assume that all user ID are in order.

2) Assume that all users use secure channels to communicate with the server, such as TLS/SSL.

3) All users and servers are honest and curious [3]. Honest and curious is defined as follows: Honest and curious users and servers will follow the protocol, but they will also try to infer other users' private data.

4) At least $m(m \geq 3)$ users participate in the federated learning process.

In this article, some parameter symbols are described as follows, as shown in Table 1.

Table 1: Symbol description

Parameter	Description
m	Number of users
d	Number of dropped users
q	Prime number in key exchange protocol
α	Additional additional mask value
w	Model parameter
$\hat{w}_j$	Model parameters masked in this article
g	Key generator

3.1 Key Exchange Protocol

The goal of the key exchange protocol is to generate a security key through negotiation by all users for parameter masking protocol. The protocol flow is as follows:

1) Initialization.

   A trusted third-party authority TA generates initialization parameters (g, q, α) for each P_j. g and q are used for key generation in the Diffie-Hellman key negotiation phase.

2) Key agreement.

   For any P_i and P_j, we take SK_i, SK_j, and compute $PK_i = g^{SK_i} mod q$, $PK_j = g^{SK_j} mod q$, broadcast PK_i, PK_j. P_i can get $S_{i,j} = PK_j^{SK_i}$ based on the received PK_j. P_j can get $S_{j,i} = PK_i^{SK_j}$ based on the received PK_i. So any two users have a common key $S_{j,i} = PK_i^{SK_j} = g^{SK_j SK_i} = PK_i^{SK_j} = S_{j,i}$. If any attacker gets $S_{j,i}$, PK_i, PK_j, g, but given the difficulty of calculating discrete logarithms, SK_i and SK_j cannot be solved.

This protocol is based on the difficulty of the discrete logarithm, so the negotiation keys of users cannot be inferred.

3.2 Association Domain Adaptive Scheme

Assume that there are two domains of data $x_i^s \in D_s$, $x_i^t \in D_t$, and a L-layer neural network embedding map $\emptyset : R^{N_0} \to R^{N_{L-1}}$, $A_i = \emptyset(x_i^s)$, $B_j = \emptyset(x_j^t)$ represent the embedding of source domain and target domain. The similarity of two samples from different domains can be expressed as the inner product $M_{ij} =< A_i, B_j >$ of A_i and B_j. The conversion probability from embedding A_i to embedding B_j is formalized as:

$$P_{ij}^{ab} = P(B_j|A_i) = \frac{exp(M_{ij})}{\sum_j exp(M_{ij})}. \tag{10}$$

The two-step round trip probability of A_i virtual random walk that starts from tagged source domain embedding A_j through an un-tagged target domain embedding B and returns to another source domain embedding A_j is expressed as:

$$P_{ij}^{aba} = (P^{ab} P^{ba})_{ij}. \tag{11}$$

Kurnia *et al.* [3] argued that high-order round-tripping would not improve performance. The two-step probability compulsion requires an approximately uniform distribution on class labels, which can be achieved by a cross entropy loss called Walker loss, i.e.,

$$L_{walker} = H(T, P^{aba}). \tag{12}$$

Where $T_{ij} = \frac{1}{|A_i|}$, if $calss(A_i) = class(A_j)$.

This means that all association loops in the same class are forced to have equal probabilities. *Walker loss* can be minimized by only accessing easily related target samples and skipping more complex target samples, which results in poor generalization of the target domain. Each target sample can be accessed with the same probability by adjusting L_{visit}. *Visit loss* is defined by the cross entropy between the uniform distribution of the target sample and the probability of access from any source sample point to the target sample point as follows:

$$L_{visit} = H(V, P^{visit}). \tag{13}$$

Where $P_j^{visit} = \sum_{x_i \in D_s} P_{ij}^{ab}$, $V_j = \frac{1}{|B|}$.

In the return mapping, the correlation is further strengthened and the coverage is increased. *Cover loss* is defined by the cross entropy between the probability of access from any target sample to the source sample and the uniform distribution of the source sample:

$$L_{cover} = H(P^{cover}, V). \tag{14}$$

Where $P_j^{cover} = \sum_{x_j \in D_t} P_{ji}^{ba}$, $V_i = \frac{1}{|A|}$. Algorithm 1 shows correlation domain adaptive (ADA) process.

3.3 Dropped Call Handling Protocol

If P_d fails to submit $\hat{w}_d$ on time due to channel failure, the w_d mask cannot be cancelled in $\hat{w}_{global}$, so the goal of the dropped line handling protocol is to eliminate the mask of the dropped user. The protocol process is as follows:

Secret sharing. The Shamir key sharing protocol is executed to divide SK_j into m parts and distribute them to m users. In the reconstruction, only the secret share of t individual is needed to reconstruct SK_j. Where t is the threshold value, $t < m$, and $t-1$ users cannot get any information about SK_j.

Key recovery. When P_d is off-line, the server requires any t users to upload the secret share of P_d. The server performs key recovery of P_d to get SK_d. The server restores the $S_{d,j} = PK_j^{SK_d}$ of P_d and P_j according to SK_d, and calculates the cover-up value $\sum_{j \in P, j<d} PRG(S_{d,j}) - \sum_{j \in P, j>d} PRG(S_{d,j})$ to eliminate the cover-up of the dropped users in the results of the aggregation model.

In conclusion, this paper proposes a new parameter masking federal learning privacy protection scheme. If there are no dropped users during the iteration, only two rounds of communication between the user and the server are needed to complete one iteration. More importantly, the server does not get the aggregated model parameters.

4 Experiment and Analysis

The deep learning model selected for experimental evaluation of the scheme in this paper is the convolutional

Algorithm 1 ADA scheme

1: **Input:** Source data x_i^s and target data x_i^t, L-layer neural network embed mapping $\emptyset$, weight factor β_1, β_2, β_3.
2: **Output:** Total neural network loss L.
3: From Formula (11), the two-step round-trip probability from source embedding A to target embedding B and back to embedding A is obtained.
4: Formula (12) is used to calculate *Walker loss*.
5: Formula (13) is used to calculate *Visit loss*.
6: Formula (14) is used to calculate the reverse random walk *Cover loss*.
7: L_{ADA} of similar embeddings between source domain and target domain is calculated according to Formulas (5,6,7) as shown in Formula (15).

$$L_{ADA} = \beta_1 L_{walker} + \beta_2 L_{visit} + \beta_3 L_{cover}. \quad (15)$$

Where, β_i is the weight factor. Equation (14) assumes that the class distribution of source and target domains is the same. If this is not the case, for L_{cover}, L_{visit}, using low weights may yield better results. At the same time, the network is trained, and the classification prediction error of the source data domain is minimized through Softmax cross entropy loss term, which is denoted as $L_{classification}$.
8: The classification prediction error $L_{classification}$ of source datax_i^s is calculated.
9: According to Equation (15), the total neural network loss L is obtained.

$$L = L_{classification} + L_{ADA}. \quad (16)$$

ADA's association loss strengthens the similar embedding assimilation of the source and target samples, and classification loss minimizes the prediction error of the source data domain. Without L_{ADA}, neural networks can only be traditionally trained on the source data domain. The addition of L_{ADA} during training allows the merging of unlabeled data from different fields, thus improving the effectiveness of classification embedding. The addition of L_{ADA} can enable any neural network to conduct domain adaptation training, and such neural network learning algorithm can simulate the distribution migration between source and target domains. If the L_{ADA} is minimized, the association embeddings from the source and target domains become more similar in their dot products.

neural network implemented by Pytorch, and the training task is handwritten digit recognition based on MNIST data set. The experimental running environment is a PC with 8-core Intel Xeon CPU and TITAN XP GPU, and the memory is 256GB. Each user runs the same model, using SGD as the optimizer. The data is randomly sampled and divided. Each user holds 60 pieces of data. In the experiment, $q = 5$, $g = 3$ and learning rate $\eta = 0.01$ are set.

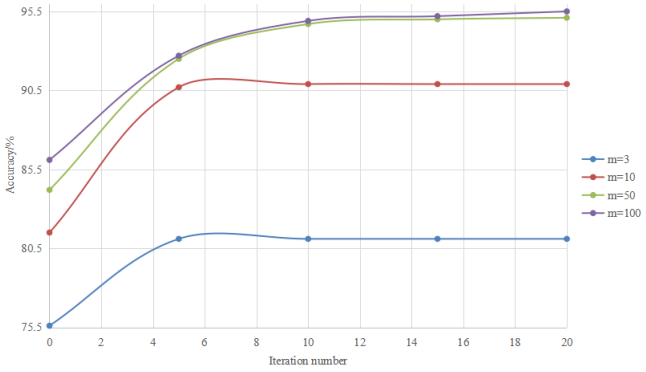


Figure 1: Accuracy evaluation of MNIST

4.1 Model Accuracy Analysis

The batch_size used in the training process is 10 and the number of local training is 10. Generally, the accuracy of the model is proportional to the number of users involved in the training. In order to analyze this relationship, this paper recorded the variation of classification accuracy of test data with the number of iterations under different users, as shown in Figure 1. Where, one iteration means one parameter update. We only consider the case where no user drops the line.

As can be seen from Figure 1, on the one hand, the classification accuracy of the model gradually increases with the increase of the number of iterations, and tends to converge after 10 iterations of training. On the other hand, when m=3, m=10, m=50 and M=100, the accuracy rate is 81.2%, 91.8%, 95.9% and 96.5%, respectively. This shows that the increase of the number of users in the system is beneficial to improve the classification accuracy of the model.

4.2 Computational Cost Evaluation

User calculation cost. The calculation cost of each user can be divided into three parts:

1) Perform m key negotiations, and the calculation cost is $O(m)$;
2) The calculation cost is $O(m^2)$ for the secret sharing of the private key;
3) To extend PRG seeds and generate model cover-up, the calculation cost is $O(zm)$. In short, the computing cost per user is $O(m^2 + zm)$.

Server computing cost. The computational cost of the server can be divided into two parts:

1) Reconstruct m secret shared values. The computational cost is $O(m^2)$ for each reconstruction and $O(m^3)$ for m reconstructions.

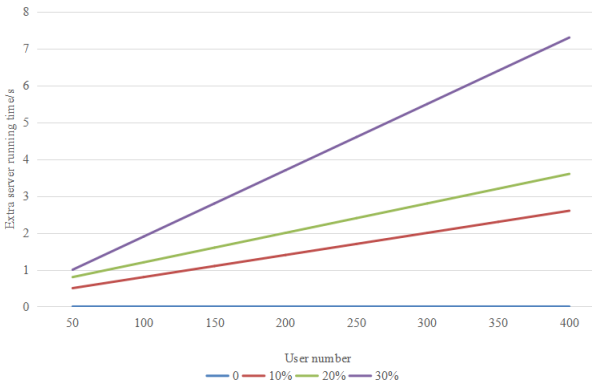


Figure 2: Additional server running time

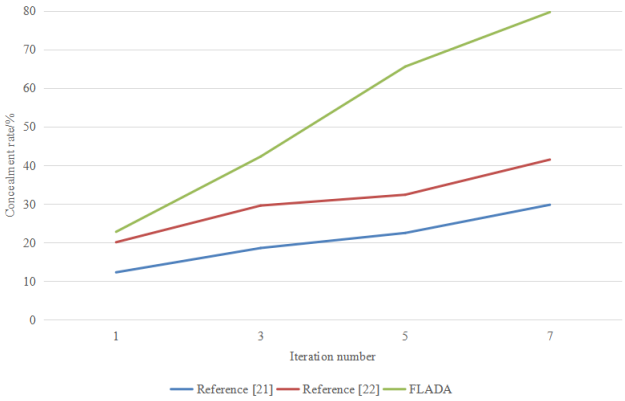


Figure 3: Comparison of hidden rate

2) Eliminate the parameter cover of the dropped user, the calculation cost is $O(zm)$. In summary, the computing cost of the server is $O(m^2 + zm)$.

4.3 Analysis of User Disconnection

Off-call evaluation mainly evaluates the impact of user off-call on the extra running time of the server. In the case of 50, 100, 150, 200, 250, 300, 350, 400 users, this article records the additional running time required for the server to perform 25 iterations with no dropouts and 10%, 20%, and 30% dropouts. The results are shown in Figure 2.

As can be seen from the results in Figure 2:

1) When the number of users is fixed, the key recovery time of the server increases with the increase of the proportion of off-line. This is because, for each dropped user, the server needs to run additional key recovery time to remove the model mask of the dropped user from the aggregated model parameters.

2) When the proportion of dropped calls is fixed, the extra running time of the server increases with the increase of the number of users. This is because as more users participate, more people drop calls and it takes longer to recover secretly. In addition, a further analysis of the data in Figure 2 shows that when the number of users is 100 and the number of dropped users is 30%, the additional server run time is around 2s, which is acceptable. In summary, based on the experimental results, it shows that the scheme in this paper can well support user disconnection.

As can be seen from Figure 3 and Table 2, after multiple iterations, the algorithm in reference [19] and the algorithm in reference [8] shows a geometric growth of the network data concealment rate, which cannot meet the requirement of network data privacy protection on the concealment rate (less than 0.6) after five iterations. The algorithm proposed in this paper increases the concealment rate of network data, but the effect is not obvious, and the concealment rate of network data is always within the required range, indicating that the algorithm proposed in this paper has a strong effect and good adaptability on the protection of network data privacy under the condition of multiple iterative updates.

Table 2: Comparison of hidden rate iteration times change with different methods

Method	1	3	5	7
Reference [25]	12.3	18.6	22.5	29.8
Reference [9]	20.1	29.6	32.4	41.5
FLADA	22.8	42.3	65.6	79.7

5 Conclusions

In order to solve the problems of parameter leakage and dependence on a trusted third party in federated learning, a new privacy protection scheme based on federated learning-association domain adaptive algorithm is proposed in this paper, which ensures that the server can only obtain the masked parameter aggregation results and can tolerate user drop-off. The security analysis proves that the scheme in this paper can effectively resist attacks from servers and users under an honest and curious security setting. Experimental results show that this scheme can guarantee the accuracy of the learning model and has lower communication cost than the existing schemes.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] S. AbdulRahman, H. Tout, H. Ould-Slimane, A. Mourad, C. Talhi, M. Guizani, "A survey on federated learning: The journey from centralized to distributed on-site learning and beyond," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5476-5497, 2020.

[2] J. Ahmed, T. N. Nguyen, B. Ali, M. Javed, J. Mirza, "On the physical layer security of federated learning based IoMT networks," *IEEE Journal of Biomedical and Health Informatics*, vol. 27, no. 2, pp. 691-697, 2022.

[3] K. Anggriani, N. Wu, M. S. Hwang, "Research on Coverless Image Steganography," *International Journal of Network Security*, vol. 25, no. 1, pp. 25-31, 2023.

[4] M. Babenko, A. Tchernykh, N. Chervyakov, V. Kuchukov, V. Miranda-López, R. Rivera-Rodriguez, Z. Du, E. G. Talbi, "Positional characteristics for efficient number comparison over the homomorphic encryption," *Programming and Computer Software*, vol. 45, pp. 532-543, 2019.

[5] M. Chamikara, P. Bertok, I. Khalil, D. Liu, S. Camtepe, "Privacy preserving distributed machine learning with federated learning," *Computer Communications*, vol. 171, pp. 112-125, 2021.

[6] J. Chen, C. Du, Y. Zhang, P. Han, W. Wei, "A clustering-based coverage path planning method for autonomous heterogeneous UAVs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 12, pp. 25546-25556, 2021.

[7] G. Dhiman, S. Juneja, H. Mohafez, I. El-Bayoumy, L. K. Sharma, M. Hadizadeh, *et al.*, "Federated learning approach to protect healthcare data over big data scenario," *Sustainability*, vol. 14, no. 5, pp. 2500, 2022.

[8] F. Dufaux, "Video scrambling for privacy protection in video surveillance: recent results and validation framework," *Mobile Multimedia/Image Processing, Security, and Applications 2011. SPIE*, vol. 8063, pp. 11-24, 2011.

[9] X. He, Q. Hu, X. Zhang, C. Zhang, W. Lin, X. Han, "Enhancing HEVC compressed videos with a partition-masked convolutional neural network," in *2018 25th IEEE International Conference on Image Processing (ICIP). IEEE*, pp. 216-220, 2018.

[10] J. Huang, C. Xu, Z. Ji, S. Xiao, T. Liu, N. Ma, Q. Zhou, "AFLPC: an asynchronous federated learning privacy-preserving computing model applied to 5G-V2X," *Security and Communication Networks*, vol. 2022, 2022.

[11] B. Jan, H. Farman, M. Khan, M. Imran, I. U. Islam, A. Ahmad, S. Ali, G. Jeon, "Deep learning in big data analytics: a comparative study," *Computers & Electrical Engineering*, vol. 75, pp. 275-287, 2019.

[12] N. M. Jebreel, J. Domingo-Ferrer, A. Blanco-Justicia, D. Sánchez, "Enhanced security and privacy via fragmented federated learning," *IEEE Transactions on Neural Networks and Learning Systems*, 2022. DOI: 10.1109/TNNLS.2022.3212627.

[13] M. Joye, P. Paillier, "Blind rotation in fully homomorphic encryption with extended keys," in *Cyber Security, Cryptology, and Machine Learning: 6th International Symposium, CSCML 2022, Be'er Sheva, Israel, June 30-July 1, 2022, Proceedings. Cham: Springer International Publishing*, pp. 1-18, 2022.

[14] A. Kammoun, R. Slama, H. Tabia, T. Ouni, M. Abid, "Generative Adversarial Networks for face generation: A survey," *ACM Computing Surveys*, vol. 55, no. 5, pp. 1-37, 2022.

[15] J. Koneny, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, D. Bacon, "Federated learning: Strategies for improving communication efficiency," *arXiv preprint arXiv:1610.05492*, 2016.

[16] A. Kumar, R. Krishnamurthi, S. Bhatia, K. Kaushik, N. J. Ahuja, A. Nayyar, M. Masud, "Blended learning tools and practices: A comprehensive analysis," *IEEE Access*, vol. 9, pp. 85151-85197, 2021.

[17] O. A. Kwabena, Z. Qin, T. Zhuang, *et al.* "Mscryptonet: Multi-scheme privacy-preserving deep learning in cloud computing," *IEEE Access*, vol. 7, pp. 29344-29354, 2019.

[18] X. Ma, F. Zhang, X. Chen, J. Shen, "Privacy preserving multi-party computation delegation for deep learning in cloud computing," *Information Sciences*, vol. 459, pp. 103-116, 2018.

[19] H. Pang, Y. Zhang, S. Wang, Y. Li, L. Sun, B. Zhang, Y. Wang, "A Novel Network Data Privacy Protection Algorithm in Big Data," *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). IEEE*, pp. 321-324, 2019.

[20] S. Rezaei, X. Liu, "Deep learning for encrypted traffic classification: An overview," *IEEE communications magazine*, vol. 57, no. 5, pp. 76-81, 2019.

[21] Z. A. Shaikh, A. A. Khan, L. Teng, A. A. Wagan, A. A. Laghari, "BIoMT modular infrastructure: The recent challenges, issues, and limitations in blockchain hyperledger-enabled e-healthcare application," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1-14, 2022

[22] Z. Tang, H. Hu, C. Xu, "A federated learning method for network intrusion detection," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 10, pp. e6812, 2022.

[23] R. Wang, W. T. Tsai, "Asynchronous federated learning system based on permissioned blockchains," *Sensors*, vol. 22, no. 4, pp. 1672, 2022.

[24] X. Wang, S. Yin, M. Shafiq, A. A. Laghari, S. Karim, O. Cheikhrouhou, W. Alhakami, H. Hamam, "A new V-net convolutional neural network based on four-dimensional hyperchaotic system for medical image encryption," *Security and Communication Networks*, vol. 2022, pp. 1-14, 2022.

[25] M. Yang, I. Tjuawinata, K. Y. Lam, "K-Means Clustering With Local d_x-Privacy for Privacy-Preserving Data Analysis," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2524-2537, 2022.
[26] M. Yang, I. Tjuawinata, K. Y. Lam, T. Zhu, "Differentially Private Distributed Frequency Estimation," *IEEE Transactions on Dependable and Secure Computing*, 2022. DOI: 10.1109/TDSC.2022.3227654.

Biography

Xiaobin Guo biography. Xiaobin Guo is with Zhengzhou Railway Vocational and Technical College, Zhengzhou City, Henan Province, 450064, China. Research interests are data security and Information encryption processing.

Guide for Authors
International Journal of Network Security

IJNS will be committed to the timely publication of very high-quality, peer-reviewed, original papers that advance the state-of-the art and applications of network security. Topics will include, but not be limited to, the following: Biometric Security, Communications and Networks Security, Cryptography, Database Security, Electronic Commerce Security, Multimedia Security, System Security, etc.

1. Submission Procedure

Authors are strongly encouraged to submit their papers electronically by using online manuscript submission at http://ijns.jalaxy.com.tw/.

2. General

Articles must be written in good English. Submission of an article implies that the work described has not been published previously, that it is not under consideration for publication elsewhere. It will not be published elsewhere in the same form, in English or in any other language, without the written consent of the Publisher.

2.1 Length Limitation:

All papers should be concisely written and be no longer than 30 double-spaced pages (12-point font, approximately 26 lines/page) including figures.

2.2 Title page

The title page should contain the article title, author(s) names and affiliations, address, an abstract not exceeding 100 words, and a list of three to five keywords.

2.3 Corresponding author

Clearly indicate who is willing to handle correspondence at all stages of refereeing and publication. Ensure that telephone and fax numbers (with country and area code) are provided in addition to the e-mail address and the complete postal address.

2.4 References

References should be listed alphabetically, in the same way as follows:
For a paper in a journal: M. S. Hwang, C. C. Chang, and K. F. Hwang, ``An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445--446, 2002.

For a book: Dorothy E. R. Denning, *Cryptography and Data Security*. Massachusetts: Addison-Wesley, 1982.

For a paper in a proceeding: M. S. Hwang, C. C. Lee, and Y. L. Tang, ``Two simple batch verifying multiple digital signatures," in *The Third International Conference on Information and Communication Security (ICICS2001)*, pp. 13--16, Xian, China, 2001.

In text, references should be indicated by [number].

Subscription Information

Individual subscriptions to IJNS are available at the annual rate of US$ 200.00 or NT 7,000 (Taiwan). The rate is US$1000.00 or NT 30,000 (Taiwan) for institutional subscriptions. Price includes surface postage, packing and handling charges worldwide. Please make your payment payable to "Jalaxy Technique Co., LTD." For detailed information, please refer to http://ijns.jalaxy.com.tw or Email to ijns.publishing@gmail.com.