# 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 $\kappa$. $p_1$ 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

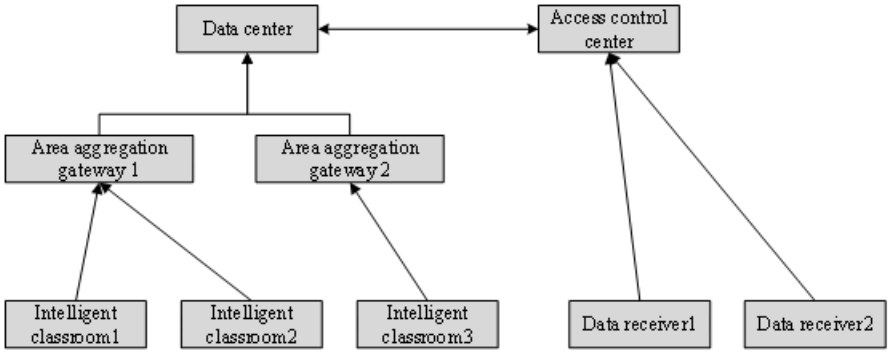


Figure 1: The proposed scheme

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 $\kappa$ and call $Gen(\kappa)$ to generate bilinear pairing parameters $(q, P, G_1, G_2, e)$. Select the security parameter $\kappa_1$ 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 $1 \times 1$ standard convolution layer are replaced by $1 \times 1$ 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 $1 \times 1$ 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 |

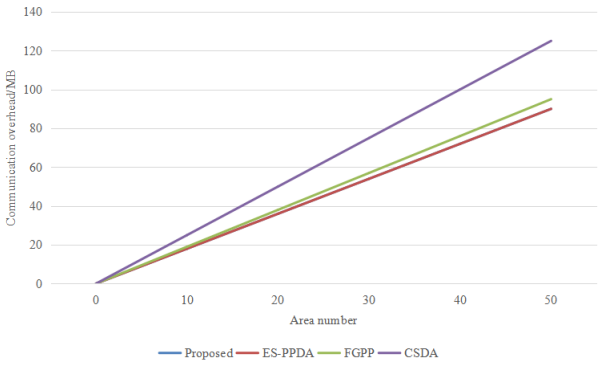


Figure 2: Comparison of the communication cost of users sent to the area aggregation gateway

# 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 |

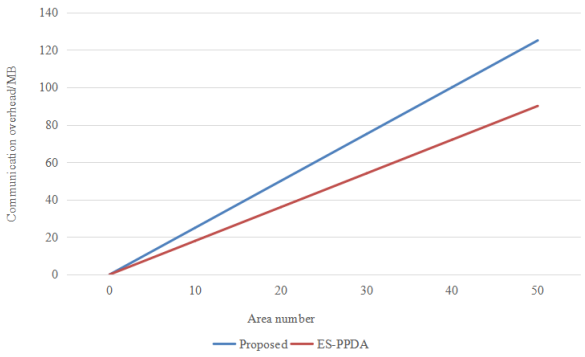


Figure 3: Comparison of the communication cost between the area aggregation gateway and the data center

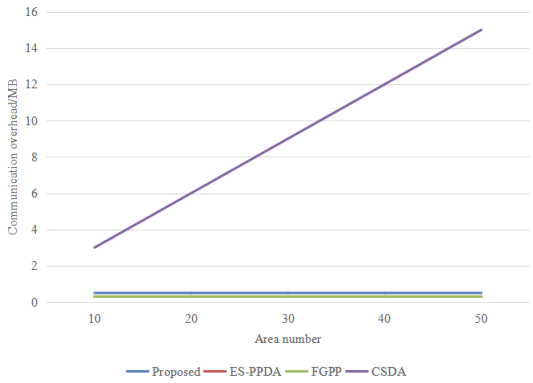


Figure 4: Comparison of communication overhead from access control Center to data receiver

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.