Security Encryption Analysis of Economic Big Data Based on Homomorphic Encryption and Attribute Base

Limin Chen

(Corresponding author: Limin Chen)

School of Finance and Economics, Zhengzhou University of Science and Technology
Zhengzhou 450064, China
Email: chenwwencww@163.com

(Received July 15, 2023; Revised and Accepted Jan. 17, 2024; First Online Feb. 23, 2024)

The Special Issue on Data Fusion, Deep Learning and Optimization Algorithms for Data Privacy Protection

Special Editor: Prof. Shoulin Yin (Harbin Institute of Technology)

Abstract

Traditional data encryption technology neglects the secondary deletion of cloud data, leading to serious redundancy of economic big data, and poor ability to resist various attacks. Therefore, in this paper, we propose a novel security encryption model based on homomorphic encryption and attribute base for economic big data. Fourier transform high-order cumulant algorithm is used to detect the duplicate data in cloud storage economy big data, and a 4-order cumulant post-processing method is selected to delete the duplicate data in the detection results. The homomorphic encryption combined with attribute-based encryption technology is used to construct an encryption scheme to complete the encryption of economy big data in cloud storage. Through theoretical analysis and experimental simulation, it is proved that the new scheme can support the access policy with rich expression ability, realize the dynamic policy update for the data in the cloud, and has advantages in storage and computing cost.

Keywords: 4-order Cumulant Post-processing Method; Attribute Base; Economic Big Data Encryption; Homomorphic Encryption

1 Introduction

At present, cloud computing services are gradually applied to various fields, and with the continuous expansion of cloud computing fields, corresponding cloud storage services appear [19]. At present, the amount of data to be stored is increasing in many fields [9], and the cloud storage mode capable of storing massive data is gradually attracting attention. Users can access the data in the cloud storage system through various forms at will. However, data loss and other phenomena may occur during the cloud storage process, and users can encrypt their own data. A layer of security service [21,23,25] is provided for data and then placed in the cloud storage server, but this method cannot fully guarantee the security of cloud storage data.

Cloud computing, the Internet of Things and the traditional industrial control system (ICS) integration, forming the industrial cloud system [11]. It connects products, factories, systems, machines, and users, and provides advanced analytics to harness the vast amounts of data generated in the network for efficiency gains and cost reductions. For a long time, enterprises pay more attention to production security and equipment security, but do not pay attention to information security and network security. This is because traditional ICS systems are proprietary, independent, and isolated from external networks [14]. In order to meet the requirements of continuous and stable production, industrial communication protocols pay more attention to the requirements of real-time, and lack the security protection of transmitted data to avoid additional costs. However, in the industrial cloud environment, the user identity is complex and diverse, and enterprises are faced with various dangers from various sources, especially the logic executed in the industrial system has a direct impact on the physical world, and the maliciously attacked system will cause serious damage and loss to human health and safety, the environment and equipment, that is, information security problems will lead to production security problems [18]. In addition, the public cloud is a semi-trusted environment, and after hosting data into a cloud storage system, enterprises cannot be sure that the storage of data is indeed protected. Therefore, it is necessary to study the confidentiality protection method in the process of data transmission, storage and sharing in the industrial cloud environment, and meet the real-time and availability requirements of indus-

trial production control.

For this reason, many scholars have studied data encryption. For example, Andola *et al.* [1] designed an encryption scheme for large data sets. For users with large data sets in the cloud storage environment, the block storage structure was used to optimize the data structure of the security index. Deng *et al.* [4] proposed a data encryption scheme capable of updating user attributes. By constructing attribute and user version key in ciphertext policy attribute encryption, the attribute version key needed to be updated when system attribute was revoked to realize the replaceable update of some components of ciphertext key. However, the encryption time of the above encryption methods is too long, and the ability to resist data attacks is weak.

In order to avoid industrial data leakage, reference [12] adopted RSA and DES encryption algorithms to prevent data from being eavesdropped during transmission and protect the security of data communication, aiming at the security of data collection in smart power plants. Aiming at the problem of secure data transmission between iot devices, reference [13] used chaotic mapping to generate AES keys and encrypt communication data, thus building a secure communication channel. In reference [26], the Paillier homomorphic encryption method was adopted to realize the secure data transmission between the field device and the controller. However, a large number of encryption and decryption operations are deployed on field sensors or actuators, which increases the computing overhead of field devices and puts forward higher requirements on network throughput. It can be seen that for ICS system, symmetric encryption scheme has low computation cost and good real-time performance, but how to manage its key is a problem that must be considered. Asymmetric encryption scheme is more secure, but the calculation cost is high, which affects the actual use. In addition, in the actual industrial cloud environment, there are many users with diverse identities, and how to ensure that users get the data within the scope of their authority and achieve fine-grained access control is also an urgent problem to be solved.

Attribute based encryption (ABE) is one of the methods for data protection and access control in cloud environment. Ciphertext-policy attribute-based encryption (CPABE) encrypts data according to the access policy and distributes the corresponding private key according to the user attributes [17]. Only the user attributes meet the requirements of the access policy. This is conceptually similar to traditional access control models such as role-based access control. Therefore, researchers are also applying CP-ABE to the industrial field to achieve data confidentiality protection and access control. References [6, 24] used CP-ABE to encrypt data and authenticate users for smart grid, medical cloud and intelligent transportation systems respectively, and only users who met the access policies in ciphertext could obtain plaintext.

Therefore, this paper studies econom big data encryption technology that supports complete outsourcing of cloud storagey. Through the improved fractional Fourier transform, duplicate data in cloud storage data was deleted to reduce the burden of data outsourcing encryption. Then, the data was outsourced to cloud storage server for attribute base and homomorphic encryption through the encryption form of complete outsourcing to the server, so as to realize data encryption and save the time of data encryption.

2 Proposed Encryption Technology

2.1 Attribute Base Encryption

When constructing the cloud storage data encryption scheme in this paper, the CP-ABE scheme under the prime-order group is taken as the basis of this research, and the theory of traditional outsourcing encryption algorithm is combined to study the verifiable fully outsourced attribute-based encryption scheme [2,5,7]. In this scheme, the following algorithms are mainly included.

1) $Setup(U) \rightarrow (pk, msk)$: The algorithm is started by AA, set the attribute set U composed of the output Y_k^M of eliminating duplicate data as the input, select the multiplicative cyclic group G, and the order of G is prime p. Let one of the generators of G be g, and randomly select $h_1, \cdots, h_U \in G$, and the exponent $a, a \in Z_p$, from which the public parameters can be obtained and expressed by Formula (1).

$$pk = (g, g^a, e(g,g)^a, h_1, \cdots, h_U). \tag{1}$$

Set $msk = g^a$ as the primary key of the cloud storage system. Where h is a random selection index. $e(g,g)$ represents the unit of G. a indicates a randomly selected integer. Z stands for bilinear set.

2) $KeyGen_{KG-CSP}(pk, S) \rightarrow (ISK_1, ISK_2)$: The algorithm is generated by two $KG - CSP$. The input of the algorithm is all attribute set S and public parameter pk. If $KG - CSP1$ starts to execute, it is necessary to select random numbers $a_1, t_1 \in Z_p$, and calculate $K' = g^{a_1} g^{at_1}$, $L' = g^{t_1}$, $\forall x \in S, K'_x = h_x^{t_1}$ to obtain the intermediate key $ISK_1 = (S, a_1, K', L', K'_{x x \in S})$ of $KG - CSP1$, the intermediate key $ISK_2 = (S, a_2, K'', L'', K''_{x x \in S})$ of $KG - CSP2$ can be obtained at the same time.

3) $KeyGen_{AA}(pk, msk, ISK_1, ISK_2) \rightarrow SK$: The algorithm is started by AA, and the inputs are set as public parameter pk, system main key msk, and intermediate key ISK_1, ISK_2. The following formulas are calculated.

$$K_1 = K' \times K'' = g^{a'} g^{at}. \tag{2}$$

$$L = L' \times L'' = g^t. \tag{3}$$

$$K_x = K'_x \times K''_x = h^t_x. \quad (4)$$

Here, $a' = a_1 + a_2$, $t = t_1 + t_2$. After calculation, the user key $SK = (S, K_1, L, K_{xx\in S}, K_2)$ is obtained, and $K_2 = g^{a-a'}$, where SK represents the user key.

4) $Encrypt(pk, msk, (M, \rho), m) \to CT$: The algorithm is executed interactively by DO and $E - CSP$. Within the access structure (M, ρ), DO encrypts the message m. Where M represents the matrix of the size of $l \times n$, and the mapping associated with each row of matrix M to the attribute is the function ρ, and ρ is the injective form. DO can randomly select the secret index $s \in Z_p$, and select the random vector $v = (s, v_2, \cdots, v_n)^T$ to make the sharing of the encryption index s more perfect. $\lambda_i = M_i v$ is calculated, where the $i - th$ row of matrix M is described by M_i; After that, DO performs operations on ciphertext $CT = ((M, \rho), C, \bar{C}, C_{ii\in[1,l]})$, in which $C = m \cdot e(g, g)^{as}, \bar{C} = g^s$. And Do algorithm for local calculation, can know $C_i = g^{a\lambda_i} h^{-s} \rho(i)$, after E-CSP cooperation calculation, can obtain C_i calculation process can be expressed by Formula (5).

$$Exp(\lambda_i, -s; g^a, h_{\rho(i)}) \to g^{a\lambda_i} h^{-s} \rho(i). \quad (5)$$

In Formula (5), λ represents the security parameter, CT represents the ciphertext, and C represents the encryption attribute.

Perform $Rand$ algorithm through DO to obtain random values (γ_1, g^{γ_1}), (γ_2, g^{γ_2}), (β, g^{β}), (a_1, g^{a_1}), (a_2, g^{a_2}), (a_3, g^{a_3}); $g^{a\lambda_i} h^{-s} \rho(i)$ is then disassembled into Formula (6).

$$g^{a\lambda_i} h^{-s} \rho(i) = g^{\gamma_1 \lambda_i - \gamma_2 s} \varpi_1^{\lambda_i} \varpi_i^{-s}. \quad (6)$$

In Formula (6), ϖ represents the outsourcing query index and γ represents the outsourcing decryption random value.

In order to ensure that the associated information will not be lost during $\varpi_1^{\lambda_i} \varpi_i^{-s}$ query, $\varpi_1^{\lambda_i} \varpi_i^{-s}$ will continue to be split and expressed by Formula (7).

$$\varpi_1^{\lambda_i} \varpi_i^{-s} = \varpi_1^{c_1,i}, \varpi_i^{c_2,i} (\varpi_1 \varpi_i^{-1})^{d_i x}. \quad (7)$$

Where d is a prime number, after the splitting is completed, the random value g^{β} is used to continue the next step of the splitting, and is expressed by Formula (8).

$$g^{a\lambda_i} h^{-s} \rho(i) = g^{\beta} g^{a_1 \zeta_1} \varpi_1^{c_1,i} \varpi_1^{c_2,i} (\varpi_1 \varpi_i^{-1})^{d_i x}. \quad (8)$$

Where $\varpi_1 = g^a / g^{\gamma_1}$, $\varpi_i = h_{\rho(i)} / g^{\gamma_2}$, $c_{1,i} = \lambda_i - d_i x$, $c_{2,i} = -s + d_i x$, $\zeta_i = (\gamma_1 \lambda_i - \gamma_2 s - \beta)$, and select $\eta_i = (a_3 - a_1 \zeta_i)/a_2$ for the next step, where β represents the random value and ζ and η represent the association information after splitting.

5) $Audit(CT^{RK}_{part}, \bar{C}, msk) \to 0/1$: The validation process is initiated by the AA authority. The algorithm input is the user decrypted value CT^{RK}_{part}, the system master key msk and the ciphertext $\bar{C}$. Analyze the size of $e(msk, \bar{C})$ and CT^{RK}_{part}, if they are equal, output "1"; If not, output "0".

2.2 Homomorphic Encryption

Assuming that the model parameter matrix of the $u - th$ $(1 \le u \le n)$ data owner is W_u, the scheme in this paper uses the Paillier algorithm to encrypt the model parameter matrix and perform homomorphism operations [3, 10, 15, 22, 27].

1) Generate public and private key pairs for encryption. First, two large prime numbers p and q are randomly selected. Note that p and q must be equal in length, and pq, $(p-1)$, $(q-1)$ are mutual primes. Second, calculate $r = pq$ and $\lambda = lcm(p-1, q-1)$, where, lcm represents the least common multiple, let $g = r + 1$. Third, let the function $L(x) = (x-1)/r$, then calculate $\mu = (L(g^{\lambda} mod(r^2)))^{-1}$. At this point, it can get the public key (r, q) and the private key (λ, μ).

2) Encrypt W_u and calculate the model parameter ciphertext c_u of the $u - th$ $(1 \le u \le n)$ data owner. First, select the random number s, where s must meet the condition $0 \le s < r$; Second, let the plaintext information corresponding to c_u be m_u, and calculate the ciphertext information $c_u = (g^{m_u} s^r) mod(r^2)$. Since $g = r + 1$, then

$$g^{m_u} = m_u r + 1 mod(r^2). \quad (9)$$

3) According to step 1 and step 2, n data owner model parameter ciphertext can be obtained, that is, $c_1, c_2, \cdots, c_n$, and the model parameter ciphertext c of the joint model computer can be obtained by performing operations in the ciphertext field, where $c = c_1 c_2 \cdots c_n$.

The joint model computer obtains the ciphertext c of the model parameter calculated in the encryption domain and decrypts it. When the ciphertext is c, $d(c)$ indicates that the ciphertext c is decrypted, that is, $d(c) = m_c$. Then the plaintext can be obtained according to Formula (6):

$$d(c) = m_c = L(c^{\lambda} mod r^2) \mu mod r. \quad (10)$$

In this paper, the homomorphism of Paillier algorithm is used to prove the feasibility of the proposed scheme. As shown in Formula (11):

$$d(c) = m_1 + m_2 + \cdots + m_n. \quad (11)$$

Table 1: Comparison of storage overhead

Method	Encryption key	Decryption key	Ciphertext of the client
HEMA	$2\|g\| + \|K_a\|$	$2\|S\|\|G\| + \|K_a\|$	$2\|G\|$
AAHE	$4\|G\| + \|K_a\|$	$(2\|S\| + 6)\|G\| + \|K_a\|$	$2\|G\| + \|Z_p\|$
HEB	$4\|U\|\|G\| + \|K_a\|$	$(2\|S\| + 3)\|G\| + \|K_a\|$	$2\|G\| + \|K_a\|$
Proposed	$\|K_a\|$	$\|Z_p\| + \|K_a\|$	$2\|G\|$

Table 2: Comparison of computing overhead

Method	Device encryption cost	Client decryption overhead
HEMA	$(2\|I\| + 1)(exp + exp_T) + \|HE\|$	$exp_T + \|HE\|\|$
AAHE	$exp_T + \|HE\|$	$exp_T + \|HE\|$
HEB	$3exp + 2exp_T + \|HE\|$	$2exp_T + e + \|HE\|$
Proposed	$\|HE\|$	$exp_T + \|HE\|$

3 Scheme Analysis

The scheme adopts a hybrid encryption method, that is, the homomorphic encryption algorithm (HE) is combined with the attribute-based algorithm (AB). The plaintext data is encrypted by HE algorithm first, and then the symmetric key K_a is encrypted by AB algorithm. Therefore, the security of symmetric key K_a determines the confidentiality of plaintext data. In this scheme, the data owner divides K_a into two sub-keys and sends them to two different fog nodes respectively. Each fog node encrypts AB algorithm independently, so each fog node does not know the symmetric key K_a of the data owner. Based on the fact that there is no collusion between different fog nodes, the fog node cannot obtain the symmetric key K_a. In addition, the symmetric key is generated by Logistic mapping in this scheme, and the key is updated after each communication between the field device and the user. Therefore, a symmetric key is only applicable to the one-time communication between the two parties. Based on the chaos of Logistic mapping, even if the attacker successfully cracks the symmetric key of a certain communication, Nor can all other keys be cracked with a non-negligible probability. In the decryption phase, the secret value s can be recovered only when the user attribute set meets the access policy, and the converted ciphertext $e(g,g)^{\frac{\alpha s}{z}}$ can be successfully decrypted. Otherwise, the decryption will be failed.

In the access policy update phase, although this part of the calculation is outsourced to the cloud, the cloud only has its selected secret value $\tilde{s}$, not the secret value s of the original file, so it cannot calculate the new secret value s' by $s' = \tilde{s} + s$. The new secret value s' is obtained by the exponential operation on the group and is hidden in the component $K_a e(g,g)^{a^{s'}}$. Because of the difficulty of calculating the discrete logarithm problem, the attacker cannot calculate s' according to the inverse operation, so the symmetric key K_a is secure.

This section compares this scheme with schemes HEMA [16], AAHE [20], and HEB [8] in terms of storage overhead and computing overhead to evaluate the performance of the scheme. The storage costs required by different schemes on the device and the client are compared, and the results are listed in Table 1. Where, $|G|$, $|G_T|$ and $|Z_p|$ represent the length of each element in G, G_T and Z_p respectively. In the symmetric bilinear pair construction, we have $|G| = |G_T|$, $|U|$ represents the number of all attributes, $|S|$ represents the number of user attributes, $|l|$ represents the number of attributes contained in the access structure, m represents the maximum number of users, and $|K_a|$ represents the length of the symmetry density.

In Table 1, the storage overhead on the device side comes primarily from encryption keys. The encryption keys of HEMA, AAHE, and HEB are composed of public key PK and symmetric key K_a, and this scheme outsources the encryption calculation of HE to the cloud and fog, so the device side of this scheme only needs to store symmetric key K_a, and the storage cost is much lower than the other three schemes.

The calculation costs of different schemes on the device and the client are compared, and the results are listed in Table 2. Let $|I|$ represent the number of user attributes matching the access policy, exp, exp_T represent the exponential operation on the group G, G_T. e represents the bilinear pair operation, and $|HE|$ represents the homomorphic encryption operation.

In the encryption process, this scheme completely outsources the encryption operation of the HE part to the cloud node [8], and only needs to perform homomorphic encryption operation on the device side, while other schemes need to complete HE and AB encryption on the device side. Therefore, the encryption cost of this scheme is small, and it is suitable for devices with limited re-

sources.

4 Conclusion

This paper studies the economy big data encryption technology of cloud storage that supports complete outsourcing, and provides perfect data for cloud storage data encryption through data deduplication algorithm. According to data homomorphic encryption technology, a data encryption scheme is constructed to realize the encryption of cloud storage data. Simulation is used to verify the effectiveness of the proposed technology, and it is proved that the encryption time and anti-attack performance of the technology are higher than other technologies.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] N. Andola, S. Prakash, V. K. Yadav, S. Venkatesan, et al, "A secure searchable encryption scheme for cloud using hash-based indexing," *Journal of Computer and System Sciences*, vol. 126, pp. 119-137, 2022.

[2] Z. Cao and O. Markowitch, "Comment on "Circuit Ciphertext-Policy Attribute-Based Hybrid Encryption With Verifiable Delegation in Cloud Computing"," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 2, pp. 392-393, 2021.

[3] S. Das, S. Namasudra, "MACPABE: Multi-Authority-based CP-ABE with efficient attribute revocation for IoT-enabled healthcare infrastructure," *International Journal of Network Management*, vol. 33, no. 3, pp. e2200, 2023.

[4] S. Deng, G. Yang, W. Dong, *et al.* "Flexible revocation in ciphertext-policy attribute-based encryption with verifiable ciphertext delegation," *Multimedia Tools and Applications*, vol. 82, no. 14, pp. 22251-22274, 2023.

[5] J. Gao, H. Yu, X. Zhu and X. Li, "Blockchain-Based Digital Rights Management Scheme via Multiauthority Ciphertext-Policy Attribute-Based Encryption and Proxy Re-Encryption," *IEEE Systems Journal*, vol. 15, no. 4, pp. 5233-5244, 2021.

[6] S. Gao, R. Wu, X. Wang, J. Liu, Q. Li, X. Tang, "EFR-CSTP: Encryption for face recognition based on the chaos and semi-tensor product theory," *Information Sciences*, vol. 621, pp. 766-781, 2023.

[7] B. Ghosh, P. Parimi and R. R. Rout, "Improved Attribute-Based Encryption Scheme in Fog Computing Environment for Healthcare Systems," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India*, pp. 1-6, 2020, doi: 10.1109/ICCCNT49239.2020.9225606.

[8] D. Han, J. Chen, L. Zhang, Y. Shen, X. Wang and Y. Gao, "Access control of blockchain based on dual-policy attribute-based encryption," in *2020 IEEE 22nd International Conference on High Performance Computing and Communications; IEEE 18th International Conference on Smart City; IEEE 6th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Yanuca Island, Cuvu, Fiji*, pp. 1282-1290, 2020, doi: 10.1109/HPCC-SmartCity-DSS50907.2020.00200.

[9] J. Hasenburg, M. Grambow and D. Bermbach, "MockFog 2.0: Automated Execution of Fog Application Experiments in the Cloud," *IEEE Transactions on Cloud Computing*, vol. 11, no. 1, pp. 58-70, 2023.

[10] J. Kim and A. Yun, "Secure Fully Homomorphic Authenticated Encryption," *IEEE Access*, vol. 9, pp. 107279-107297, 2021.

[11] S. Maesschalck, V. Giotsas, B. Green, N. Race, "Don't get stung, cover your ICS in honey: How do honeypots fit within industrial control system security," *Computers & Security*, vol. 114, pp. 102598, 2022.

[12] D. O. Orucho, F. M. Awuor, R. Makiya, C. Oduor, "Review of Algorithms for Securing Data Transmission in Mobile Banking," *Modern Economy*, vol. 14, no. 9, pp. 1192-1217, 2023.

[13] Z. Rahman, X. Yi, M. Billah, M. Sumi, A. Anwar, "Enhancing AES using chaos and logistic map-based key generation technique for securing IoT-based smart home," *Electronics*, vol. 11, no. 7, pp. 1083, 2023.

[14] Y. Su, M. Zhao, C. Wei, X. Chen, "PT-TODIM method for probabilistic linguistic MAGDM and application to industrial control system security supplier selection," *International Journal of Fuzzy Systems*, pp. 1-14, 2022.

[15] L. Teng, H. Li, J. Liu, S. Yin, "An efficient and secure cipher-text retrieval scheme based on mixed homomorphic encryption and multi-attribute sorting method under cloud environment," *International Journal of Network Security*, vol. 20, no. 5, pp. 872-878, 2018.

[16] R. Thenmozhi, S. Shridevi, S. N. Mohanty, V. Garcìa-Dìaz, D. Gupta, P. Tiwari, M. Shorfuzzaman, "Attribute-based adaptive homomorphic encryption for big data security," *Big Data*, 2021. ahead of print, http://doi.org/10.1089/big.2021.0176

[17] H. Wang, J. Liang, Y. Ding, S. Tang, Y. Wang, "Ciphertext-policy attribute-based encryption supporting policy-hiding and cloud auditing in smart health," *Computer Standards & Interfaces*, vol. 84, pp. 103696, 2023.

[18] X. Wang, Y. Sun, D. Ding, "Adaptive dynamic programming for networked control systems under communication constraints: a survey of trends and tech-

niques," *International Journal of Network Dynamics and Intelligence*, pp. 85-98, 2022.

[19] C. Wu, A. N. Toosi, R. Buyya and K. Ramamohanarao, "Hedonic Pricing of Cloud Computing Services," *IEEE Transactions on Cloud Computing*, vol. 9, no. 1, pp. 182-196, 2021.

[20] Z. Xu, S. Cao, "Multi-Source Data Privacy ProtectionMethod Based on Homomorphic Encryption and Blockchain," *CMES-Computer Modeling in Engineering & Sciences*, vol. 136, no. 1, 2023.

[21] 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.

[22] X. Yang, S. Zheng, T. Zhou, Y. Liu and X. Che, "Optimized relinearization algorithm of the multikey homomorphic encryption scheme," *Tsinghua Science and Technology*, vol. 27, no. 3, pp. 642-652, 2022.

[23] S. Yin, H. Li, S. Karim, and Y. Sun, "ECID: Elliptic Curve Identity-based Blind Signature Scheme," *International Journal of Network Security*, vol. 23, no. 1, pp. 9-13, 2021.

[24] S. Yin, H. Li, L. Teng, A. A. Laghari, V. V. Estrela, "Attribute-based Multiparty Searchable encryption model for Privacy Protection of Text Data," *Multimedia Tools and Applications*, 2023. ttps://doi.org/10.1007/s11042-023-16818-4.

[25] S. Yin, J. Liu and L. Teng, "Improved Elliptic Curve Cryptography with Homomorphic Encryption for Medical Image Encryption," *International Journal of Network Security*, vol. 22, no. 3, pp. 419-424, 2020.

[26] Z. P. Yuan, P. Li, Z. -L. Li, J. Xia, "A Fully Distributed Privacy-Preserving Energy Management System for Networked Microgrid Cluster Based on Homomorphic Encryption," *IEEE Transactions on Smart Grid*, 2023. doi: 10.1109/TSG.2023.3309405.

[27] C. Zhou and N. Ansari, "Securing Federated Learning Enabled NWDAF Architecture with Partial Homomorphic Encryption," *IEEE Networking Letters*, 2023. doi: 10.1109/LNET.2023.3294497.

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.