Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 8810987, 9 pages
https://doi.org/10.1155/2020/8810987

WILEY | Hindawi

Research Article

A New Private Information Encryption Method in Internet of Things under Cloud Computing Environment

Haiyun Ma[1] **and Zhonglin Zhang**[2]

[1]*School of Electronic Information and Electrical Engineering, Tianshui Normal University, Tianshui 741001, China*
[2]*School of Electronic and Information Engineering, Lanzhou Jiaotong University, Lanzhou 730070, China*

Correspondence should be addressed to Haiyun Ma; mhytsnu@163.com

Received 7 May 2020; Revised 26 August 2020; Accepted 27 August 2020; Published 15 September 2020

Academic Editor: Omprakash Kaiwartya

The existence of Internet of Things (IoT) facilitates the collection and transmission of urban data information. However, it can leak users' personal privacy information in smart cities. Therefore, we propose a new private information encryption method in IoT under cloud computing environment. Under IoT, according to the properties and acquisition time, privacy information can be divided into many subspaces. Then, we analyze the private information encryption with different levels. Based on the stream cipher mechanism, we design an encryption system model of information collection. In the subspace, the privacy information is encrypted and transferred to the relay node. After encrypting, they are segmented and restructured. The long privacy information is divided into smaller slices. Then, they are reintegrated after conversion. Finally, we use stream cipher and dual-key algorithm to complete freedom nondestructive transformation between plaintext and ciphertext to ensure the integrity of the encrypted private information. Experimental results show that the proposed method takes less time in the encryption and decryption process, which has better ciphertext conversion output effect and suffers fewer network attacks in the same encryption time. The message encryption and decryption time is less than that of other methods. In terms of calculation cost, the proposed method decreases by approximately 14%. What is more, it has higher security and improves the security and integrity of the privacy information collection process.

1. Introduction

Increasing quantities of data are being generated and stored from our daily lives, leading to a rise in big data analytics. Our research focuses on urban data encryption technologies that are aimed at using the big urban data sets generated as people live, work, and move around a city. The Internet of Things (IoT) [1] is a great development of Internet interconnection technology after the Internet. It is no longer the interconnection between users in the simple sense, but the connection between things. But the development of the mobile Internet is faced with many problems, such as in the private process of information collection and transmission security encryption, which is needed to be solved. With the rapid development and wide application of mobile Internet technology and communication technology, interconnection makes the acquisition and application of private information become more agile [2, 3]. Due to the mobile Internet, information collection is easily invaded and attacked by malicious data in terms of stability or faces the risk of data being stolen. While network users enjoy timely and convenient personalized services, they usually need to disclose personal privacy information in exchange for corresponding services. Therefore, under the condition of IoT, the collection and transmission of information should be encrypted to ensure the security of the information system. Mobile Internet technology and communication technology have been rapidly developed and widely applied in private information encryption. The users enjoy convenient and personalized services but usually need to disclose personal privacy information as the price for the corresponding service at the same time. Private data owners that provide users with better quality of service must understand the users' own sensitive information, the privacy information, and the contradiction between privacy

information disclosure and the quality of service [4–6]. Privacy information security has gradually become a common concern of mobile Internet users and is also related to the Internet urgent problems for managers. Meanwhile, the owner of privacy data must understand users' own sensitive information, which results in the contradiction between privacy information disclosure and service quality.

Elgendy et al. [7] proposed a novel framework to offload intensive computation tasks from the mobile device to the cloud. This framework used an optimization model to determine the offloading decision dynamically based on four main parameters, namely, energy consumption, CPU utilization, execution time, and memory usage. In addition, a new security layer was provided to protect the transferred data in the cloud from any attack. But this work cannot process tasks in parallel. Karthikeyan et al. [8] presented key exchange techniques based on secured energy efficiency in mobile cloud computing. The cloud providers must take strong security measures to protect the integrity and privacy of the healthcare-related data. But most of the researchers do not simultaneously pay attention to both integrity and privacy for Health-CPS. Therefore, Xu et al. [9] proposed a privacy-preserving data integrity verification model by using lightweight streaming authenticated data structures for Health-CPS. Elgendy et al. [10] presented a multiuser resource allocation and computation offloading model with data security to address the limitations of such devices. The computation and radio resources were jointly considered for multiuser scenarios to guarantee the efficient utilization of shared resources. Haseeb et al. [11] presented a Secure Sensor Cloud Architecture (SASC) for IoT applications to improve network scalability with efficient data processing and security. The proposed architecture comprised two main phases. Firstly, network nodes were grouped using unsupervised machine learning and exploited weighted-based centroid vectors for the development of intelligent systems. Secondly, the proposed architecture made use of sensor-cloud infrastructure for boundless storage and consistent service delivery. For the computational overhead and signature efficiency issues of traditional signature mechanisms, Zhu et al. [12] proposed a scheme of data integrity verification based on a short signature algorithm, which supported privacy protection and public auditing by introducing a trusted third party.

In the field of security encryption and transmission of mobile Internet data collection, many domestic and foreign scholars have conducted relevant exploration and research, mainly including symmetric information encryption technology represented by DES and [13] AES [14] and asymmetric information encryption technology represented by RSA [15].

These encryption technologies can realize the encrypted collection and transmission of Internet information according to the key management of the sender and the receiver. However, the calculation process of these existing encryption technologies is too complex, which requires higher suitability for application scenarios, and the security of overall data encryption needs to be improved. In order to solve the network users' privacy information leakage problem, Zhang and Luo [16] put forward an encryption method based on metadata attributes. This method used the metadata attributes of privacy information object to evaluate data value of privacy information and classified the private information. According to the value level of privacy information, it selected the corresponding encryption method and gave privacy information encryption solution. But it ignored the integrity of the privacy information acquisition process resulting in the poor information encryption effect. Liu et al. [17] proposed a data encryption method based on dynamic key in the process of privacy information collection. This method adopted the retransmission packet synchronization updating the key of both sides. It used XOR algorithm to complete privacy information symmetry encryption. The keys and privacy information were as the input of the Hash algorithm. The Hash value was as the message digest to complete privacy information integrity authentication. This method effectively ensured the integrity of privacy information in acquisition process. However, the time and space complexity was higher. Wei-Wei [18] presented a research on information acquisition and encryption based on spatial-temporal chaos. The encryption level of information was analyzed, and the sequence generation process and density distribution of spatial-temporal chaotic encryption technology were studied. The information collection and encryption process under the condition of spatial-temporal chaotic encryption was given. Based on the stream cipher mechanism, the system encryption model was designed. Finally, the stream cipher and double-key algorithm were used. It completed the conversion between plaintext and ciphertext and realized the secure collection and transmission of information under the condition of mobile Internet. Sedghi et al. [19] proposed a generic model for the analysis of searchable encryption. Then, it identified the security parameters of searchable encryption schemes and proved information theoretical bounds on the security of the parameters. Yi et al. [20] showed that the customized data container (CDC) into DIBE (diffractive-imaging-based encryption) was introduced and a new phase retrieval algorithm (PRA) for plaintext retrieval was proposed. The PRA, designed according to the peculiarity of the CDC, combined two key techniques from previous approaches, i.e., input-support-constraint and median filtering. The proposed scheme could guarantee totally the reconstruction of the primary information despite heavy noise or occlusion, and its effectiveness and feasibility had been demonstrated with simulation results. However, some demerits are still in their schemes.

To solve the above problems, we propose a new private information encryption method in Internet of Things under cloud computing environment. The flow chart of secure encryption information acquisition is shown in Figure 1.

Our main contributions are as follows:

(1) Mobile Internet privacy information can be divided into several subspaces according to its properties and acquisition time

(2) All the encrypted privacy information is transmitted and stored in network relay node

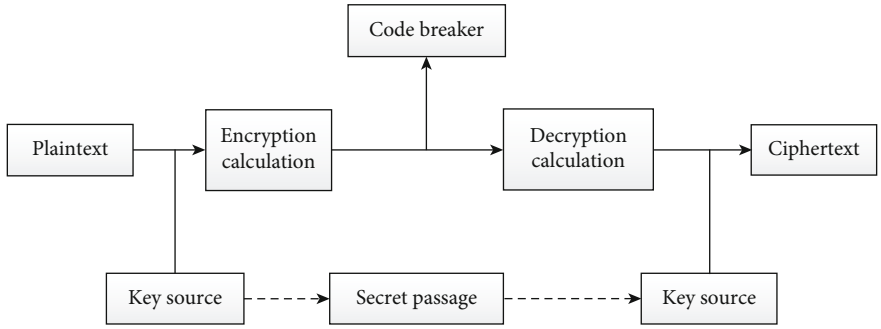

Figure 1: Secure encryption information acquisition process.

(3) When the node needs to read the privacy information, the data source node is required to request the corresponding subkey for the privacy information

(4) The data source node determines whether to generate and return the appropriate child keys based on its policy

On the basis of the privacy information encryption method [21–23] via acquisition time, this paper introduces the segmentation and reorganization technology to divide the lengthy privacy information into smaller information slices and then integrates them after conversion. In addition, the mobile Internet node authentication is added to increase the effectiveness and reliability of the source of privacy information.

This paper is organized as follows. Section 2 gives the encryption hierarchy analysis in privacy information collection process. We introduce the information collection process encryption based on stream cipher in Section 3. Integrity optimization of privacy information encryption is verified in Section 4. Section 5 shows the experiments and results. There is a conclusion in Section 6.

2. Encryption Hierarchy Analysis in Privacy Information Collection Process

Under the cloud computing, information collection, acquisition, and transmission are more convenient. Encryption and security processing in information collection usually include three levels, namely, end-to-end encryption, encryption between nodes, and link encryption [24–26]. The hierarchy between data acquisition and transmission ensures the security of information acquisition to a large extent. Link encryption encrypts the communication path between two communication nodes and provides security authentication for data collection and transmission. Before collecting and transmitting link information, the nodes in sending and transmitting need to be encrypted. This information encryption method is usually used for the conversion of synchronous and asynchronous lines. The encryption processing of devices at both ends of the link should be carried out synchronously to improve the security of information acquisition [27]. However, this encryption method requires frequent conversion of encryption devices, increasing the risk of loss in data collection.

Node encryption can increase the security of information collection. But for the intermediate nodes, it needs to decrypt and encrypt frequently. It is too complex and has high cost [28], because it will process all the node information in the link path. So the whole process of data collection requires transparency to users, which also increases the risk of information acquisition. End-to-end information encryption method has certain advantages, but some defects are still in encryption performance.

The plaintext of privacy information collection process is encrypted by bit operation. The number of iterations is large, and the encryption efficiency will decrease with the increase of the plaintext of privacy information. The plaintext is divided into many blocks, and each block generates an iterative sequence with different initial values separately. Encryption can effectively solve this problem, and the specific process is described below.

The privacy information is divided into n blocks in the plaintext; the size of each block is l_i. L is the length of the plaintext, and the chunking strategy is as follows: the former $n-1$ blocks with equal length of privacy information is $4N$, and the nth block is the rest of the privacy information, that is,

$$l_i = \begin{cases} 4N(i < N), \\ L - 4N(n-1)\ (i = n). \end{cases} \tag{1}$$

For each plaintext block, according to the Lorenz chaos mapping and Chen chaotic map, it generates the initial value and interference value. In the process of each iteration, it produces a random sequence value containing two random sequences, namely, the chaotic sequence value $x = (x_1, \cdots, x_6)$. The offset θ_i of the first character gets private information. ρ_t denotes the iteration number of the Lorenz chaotic system. N_0 represents the initial iteration number of the Chen chaotic system. So the total iteration number ρ is

$$\begin{aligned} \rho_{\mathrm{L}} &= \theta_i / N + N_0, \\ \rho_{\mathrm{C}} &= \theta_i / N + M_0. \end{aligned} \tag{2}$$

The following formula can be used to calculate the corresponding chaotic sequence of each plaintext block.

$$\chi_\rho = (x_1(\rho_{\mathrm{L}}), x_2(\rho_{\mathrm{L}}), \cdots, x_6(\rho_{\mathrm{L}}), x_1(\rho_{\mathrm{C}}) \cdots, x_6(\rho_{\mathrm{C}})). \tag{3}$$

In order to make the chaotic sequence generated by the Lorenz chaotic system and Chen chaotic system have coupling, we use the following formulas:

$$\begin{aligned} x_4(\rho_C) &= x_4(\rho_C) \oplus x_1(\rho_L), \\ x_5(\rho_C) &= x_5(\rho_C) \oplus x_2(\rho_L), \\ x_6(\rho_C) &= x_6(\rho_C) \oplus x_3(\rho_L). \end{aligned} \tag{4}$$

The corresponding chaotic sequence χ_ρ of two chaotic systems is divided into initial value sequence χ_ρ^l and interference sequence χ_ρ^d.

$$\begin{aligned} \chi_\rho^l &= (x_1(\rho_L),\cdots,x_4(\rho_C)), \\ \chi_\rho^d &= (x_5(\rho_C), x_6(\rho_C)). \end{aligned} \tag{5}$$

The initial value sequence χ_ρ^l can be regarded as the plaintext encryption sequence $\omega_\rho = (\omega_1(\rho),\cdots,\omega_4(\rho))$ recursion generated by the initial value of two chaotic systems. The interference sequence makes a second interference for the privacy information ciphertext to enhance the security. To make more coupling between the Lorenz chaotic system and Chen chaotic system, we use the following equations:

$$\begin{aligned} \omega_3(\rho) &= \omega_1(\rho) \oplus \omega_3(\rho), \\ \omega_4(\rho) &= \omega_2(\rho) \oplus \omega_4(\rho). \end{aligned} \tag{6}$$

After obtaining the encryption sequence, it is not possible to perform XOR operation with the private information in the plaintext, and the plaintext encryption sequence needs to be converted into a certain module space by using the following formulas:

$$\begin{aligned} \omega_i(\rho) &= \text{mod}\ (|\omega_i(\rho)| - \lfloor \omega_i(\rho) \rfloor) \times 10^9, \\ x_i(\rho) &= \text{mod}\ (|x_i(\rho)| - \lfloor x_i(\rho) \rfloor) \times 10^9. \end{aligned} \tag{7}$$

After preparing plaintext encryption sequence, the encryption operation is performed. This process is aimed at randomly selecting multiple bytes in the plaintext block of privacy information to obtain its corresponding ASCII code M. XOR operation with the encryption sequence will obtain intermediate results. And on this basis, XOR operation with the interference sequence will obtain the final ciphertext C of privacy information.

$$\begin{aligned} C_{4k+1} &= M_{4k+1} \oplus \omega_1(k+1) \oplus x_5(k+1), \\ C_{4k+2} &= M_{4k+2} \oplus \omega_2(k+1) \oplus x_6(k+1), \\ C_{4k+3} &= M_{4k+3} \oplus \omega_3(k+1) \oplus x_4(k+1), \\ C_{4k+4} &= M_{4k+4} \oplus \omega_4(k+1) \oplus x_6(k+1), \end{aligned} \tag{8}$$

where $k+1$ represents the iteration number of the encrypted mixed chaotic system in the privacy information collection process.

3. Information Encryption Based on Stream Cipher

The private information encryption process under the condition of mobile Internet is composed of plaintext message space, encryption calculation, ciphertext message space, and decryption result.

For a given information collection plaintext and key, the plaintext should be firstly converted into ciphertext by an encryption algorithm. When the information receiver receives the ciphertext, the key source is obtained through the secret channel. And then, the ciphertext is converted into plaintext by a decryption algorithm. In ciphertext parsing, the appropriate key conversion function can be selected.

However, network attackers often take measures to intercept the ciphertext and obtain a certain element in the plaintext space. Therefore, under the condition of cloud computing, the information encryption system can classify and control the ciphertext based on three independent perspectives. In the context of cloud computing, encryption process of information collection based on chaos technology should follow the basic operating rules, namely, replacement rules and decryption rules. Every element in the plaintext information, such as sound, document, and image, is mapped and transformed into a ciphertext element according to certain password rules. The ciphertext information has been rearranged and combined to replace the plaintext information with ciphertext information.

Decryption based on chaotic technology improves the efficiency of data collection, encryption, and decryption. It reduces the risk of theft and disclosure during information distribution and storage. In essence, the setting of this mechanism is to improve the security of information collection and encryption and reduce the hidden danger of data security brought by the same key. Besides a public key, every mobile network user also holds a private key. The encryption technology based on chaotic information has higher security, smaller storage space, and lower requirements than traditional technology. According to the requirements of plaintext processing, the plaintext information is encrypted step by step according to the sequence of characters based on stream cipher by chaos technology [29–32].

Under the condition of the cloud computing, it uses the stream cipher to encrypt the sequence based on the characters in the process of information encryption process. In the conversion of plaintext and ciphertext, the bidirectional coupling image lattices and randomness test methods are used to verify the generated sequence values, so as to determine whether the sequence values of the chaotic technique match the stream cipher. In the process of transforming ciphertext into plaintext, the original plaintext information can be completely recovered by processing ciphertext signal as input value. The length of sequence value in a stream cipher scheme is adjustable, and the length of chromium point in key distribution will affect ciphertext conversion. The security level of stream cipher will determine the security of the plaintext information and the length of the containing characters.

4. Integrity Optimization of Privacy Information Encryption

Based on the privacy information encryption of acquisition time, we introduce segmentation recombinant technology, and the lengthy privacy information is divided into smaller slices. Fusion is performed after conversion. Mobile Internet node authentication is added to increase the validity and reliability of privacy information sources. The specific process is described as below.

Assume that η represents the nodes of the mobile Internet. The network node randomly selected S_η, $J = |S_\eta|$, using h hop. One of the nodes η randomly divides the detected privacy information into κ patches. The network node η retains only one patch and transmits the remaining $\kappa - 1$ slices of privacy information to the rest of the nodes of the mobile Internet using an encrypted method.

Suppose that the Internet node η transmits $d_{\eta'\kappa'}$ privacy information to the node κ. The final aggregation result of the privacy information can be expressed as follows:

$$f = \sum_{\kappa}^{N} d_{\eta'} = \sum_{\kappa}^{N} \sum_{\eta}^{N} d_{\eta'} d_{\eta'\kappa'} = 0. \tag{9}$$

When the node η of the mobile Internet has received the slices of encrypted privacy information of the remaining nodes, the subkeys of the nodes are used to decrypt them until the slices of privacy information of the remaining nodes are received. A weighted sum of them is conducted. Then we get

$$r_{\kappa'} = \sum_{\kappa'}^{N} d_{\eta'\kappa'} d_{\eta'\kappa'} = 0. \tag{10}$$

The aggregation privacy information of all mobile Internet nodes will transmit the final result to the sink node, so,

$$\sum_{\kappa'}^{N} r_{\eta'} = \sum_{\kappa=1}^{N} \sum_{\eta=1}^{N} d_{\eta'\kappa'}. \tag{11}$$

Privacy protection in the process of privacy information collection is realized by the privacy information recombination and aggregation. The aggregated privacy information is finally uploaded to the sink node, restoring the original privacy information and achieving the purpose of privacy protection.

5. Experimental Results and Analysis

In order to verify the comprehensive effectiveness of the proposed method, we conduct comparison experiments with BKG [33], ACBE [34], and DSSE [35] in terms of safety, integrity, and computational complexity. The experiment condition is Intel® Core™ i7-6700 CPU @ 3.40 GHz–3.41 GHz, Matlab 2017a.

Table 1: Key number comparison.

Iteration number	BKG	ACBE	DSSE	Proposed
8	645	623	579	130
16	668	646	612	155
24	701	679	645	188
32	1152	1568	987	245

Table 2: Calculation comparison.

Index	BKG	ACBE	DSSE	Proposed
PE%	38.72	38.55	34.38	15.83
AO%	85.47	84.79	79.64	59.41

Table 3: Key number comparison.

Information data	BKG	ACBE	DSSE	Proposed
200	13.5	26.7	35.8	50.1
400	25.6	58.7	59.4	71.4
600	58.8	71.6	73.4	85.6
800	69.3	84.3	87.9	96.4

The security of privacy information is often reflected by the antiaggressiveness in the collection process, which is directly related to the number of subkeys. Table 1 shows the key number with different methods which illustrates the encryption safety.

When the proposed method encrypts and transmits privacy information in the subspace, it needs to request the corresponding subkey of privacy information from the data source node. The data source node decides whether to authorize or not according to its own policy.

It can be seen from Table 1 that when the subkey number is 188 of the proposed method, the security performance of privacy information acquisition encryption is the same as BKG (701), ACBE (679), and DSSE (645). It can be concluded from the above analysis that under the same security performance condition, the method in this paper generates the minimum number of subkeys, which proves that it has a high security performance.

Table 2 displays the actual amount of encrypted privacy information data and additional overhead. PE% shows the proportion of encrypted data. AO% shows the additional overhead.

According to the analysis of Table 2, when using the method in this paper to encrypt private information, the additional cost caused by subspace division, information encryption transmission time, and data source node authorization is about 60%, which means that the extra cost is longer than the actual time of privacy information encryption operation. However, the BKG, ACBE, and DSSE methods have more costs, accounting for 85.47%, 84.79%, and 79.64%, respectively. In terms of the proportion of actual encrypted private data, since the BKG method uses nonretransmission data packets to update the key of both parties

Table 4: Message encryption and decryption.

Process	"I was rich"	"It is difficult"
Encoded output	TCGGCTGCTGCACTACCTTGTCGTAA GACCTGGAAGTACC	CAAAACCCATCACCAAAACGCAACTTCGTCGTTAGTTGAAT TGTAACAAGAGGGCTTCAGTTCGTAATAATGGATCATAG
Decoded output	GCCTTTGCGCCCAAGGTGTCATGGAG TTAACAACACATAC	AAGCGCCCCACCATGTGCCCTGAATAAAGAACCCGAAAC ATCCCTCTACATCGCGGGCTAGCACCATGTAAGGTACATGT
Retrieved message	"I was rich"	"It is very difficult"
Total time	0.2583 s	0.1357 s

synchronously and adopts the XOR algorithm to complete symmetric encryption and decryption of privacy information, the actual amount of encrypted privacy data is large, reaching to 38.72%.

When the privacy information is encrypted by the proposed method, the privacy information is encrypted in the subspace and transmitted to the relay node. When the relay node needs to read the privacy information, only the child keys are generated for some data source nodes, and the total amount of actually encrypted privacy data is only 15.83%. The experimental results show that the proposed privacy encryption in this paper has low computational complexity.

BKG does not design the protection measure in the privacy information collection, which can lead to the loss of part of the encrypted privacy information. But in the new method, the information encrypted by segmentation and restructuring, the lengthy privacy information is divided into smaller slices. Through the integration of the reentry after conversion, it effectively guarantees the privacy information integrity in the process of polymerization. The comparison of the different methods is shown in Table 3.

It can be seen from the Table 3 that with the increasing amount of privacy information data, the integrity of information encrypted by different methods is higher. However, the new method in this paper is superior to other methods, mainly because the new method introduces authentication strategy, which can effectively ensure the integrity of privacy information in the IoT.

And message encryption and decryption processes are proved with our proposed scheme. We input two messages "I was rich" and "It is very difficult." Table 4 is the result. It shows that the proposed method can encrypt and decrypt message accurately.

We also study the network malicious attack for security encryption in information collection process as shown in Table 5.

Table 5 shows the network attack number based on the four encryption technologies in different encryption times. At different encryption time points, the network attack number with the proposed encryption technology in this paper is the lowest, which also verifies the robustness of the encryption technology proposed in this paper.

In addition to analyzing the efficiency of information security, this paper also compares and verifies the information collection and transmission effects of encryption technology. The selected comparison technology is RSA encryption technology. Figure 2(a) shows the original plaintext image, and Figure 2(b) shows the encrypted image with the proposed method. It can be seen that the proposed encryption has good effect under cloud computing environment, with high security and confidentiality.

Table 5: Attack number comparison.

Encryption time (s)	BKG	ACBE	DSSE	Proposed
20	29	23	20	12
40	37	33	28	16
60	42	38	31	18
80	48	42	35	20
100	52	47	37	21
120	53	50	39	22
140	58	55	43	23
160	61	57	46	24
180	65	59	48	25
200	67	61	50	26

Figure 3(a) shows the effect of image decrypted by the new method, which is true and clear; it is consistent with the detailed information and display effect of the original image. Figure 3(b) shows the decryption effect processed by RSA technology. After comparison with the original image, it is found that some details are missing, and the gray-level information of the image is inconsistent with the original image.

The main reason for this situation is that the RSA technology does not adopt double-key decryption. In order to provide security to extend the length of the encoding, it leads to the inconsistency of some image character information before and after encryption. However, the encryption technology proposed in this paper has a very high security, changing the sequence length before and after the encryption of information, and has a high security. The original image is obtained from the decoded information without losing any detailed information. In the process of decryption, the MDS file is restored, and it improves the security and reliability of the decoded image.

6. Conclusions

Because chaotic algorithm has no obvious symmetry and periodicity requirement, it is more concise in problem processing, so it is very suitable for private information encryption. Chaos has rich hierarchical structure characteristics. This paper makes full use of the advantages of chaos technology to improve the security of mobile Internet users'

(a) (b)

Figure 2: Original image and encrypted image.

(a) (b)

Figure 3: Image decryption.

information collection and output. Then, we use stream cipher and dual-key algorithm to complete freedom nondestructive transformation between plaintext and ciphertext to ensure the integrity of the encrypted information. The experimental result proves the superiority of the proposed encryption technology. In the future, more deep learning methods will be applied to the private information encryption. And they will be applied to practical projects.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the Natural Science Foundation of Gansu Province of China (18JR3RE245).

References

[1] Q. Zhang, L. T. Yang, Z. Chen, and P. Li, "High-order possibilistic c-means algorithms based on tensor decompositions for big data in IoT," *Information Fusion*, vol. 39, pp. 72–80, 2018.

[2] P. Li, Z. Chen, L. T. Yang, L. Zhao, and Q. Zhang, "A privacy-preserving high-order neuro-fuzzy c-means algorithm with cloud computing," *Neurocomputing*, vol. 256, pp. 82–89, 2017.

[3] S. Yin and J. Liu, "A K-means approach for map-reduce model and social network privacy protection," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 6, pp. 1215–1221, 2016.

[4] J. Liu, S. Yin, H. Li, and L. Teng, "A density-based clustering method for K-anonymity privacy protection," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 8, no. 1, pp. 12–18, 2017.

[5] L. Meng, S. Yin, C. Zhao, H. Li, and Y. Sun, "An improved image encryption algorithm based on chaotic mapping and discrete wavelet transform domain," *International Journal of Network Security*, vol. 22, no. 1, pp. 155–160, 2020.

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

[7] I. Elgendy, W. Zhang, C. Liu, and C. Hsu, "An efficient and secured framework for mobile cloud computing," *IEEE Transactions on Cloud Computing*, 2018.

[8] B. Karthikeyan, T. Sasikala, and S. B. Priya, "Key exchange techniques based on secured energy efficiency in mobile cloud computing," *Applied Mathematics & Information Sciences*, vol. 13, no. 6, pp. 1039–1045, 2019.

[9] J. Xu, L. Wei, W. Wu, A. Wang, Y. Zhang, and F. Zhou, "Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber-physical system," *Future Generation Computer Systems*, vol. 108, pp. 1287–1296, 2020.

[10] I. A. Elgendy, W. Zhang, Y. C. Tian, and K. Li, "Resource allocation and computation offloading with data security for mobile edge computing," *Future Generation Computer Systems*, vol. 100, pp. 531–541, 2019.

[11] K. Haseeb, A. Almogren, I. Ud Din, N. Islam, and A. Altameem, "SASC: secure and authentication-based sensor cloud architecture for intelligent Internet of Things," *Sensors*, vol. 20, no. 9, p. 2468, 2020.

[12] H. Zhu, Y. Yuan, Y. Chen et al., "A secure and efficient data integrity verification scheme for cloud-IoT based on short signature," *IEEE Access*, vol. 7, pp. 90036–90044, 2019.

[13] S. F. Chiou, M. S. Hwang, and S. K. Chong, "A simple and secure key agreement protocol to integrate a key distribution procedure into the DSS," *International Journal of Advancements in Computing Technology*, vol. 4, no. 19, pp. 529–535, 2012.

[14] C. H. Wei, M. S. Hwang, and A. Y. H. Chin, "An improved authentication protocol for mobile agent device in RFID environment," *International Journal of Mobile Communications*, vol. 10, no. 5, pp. 508–520, 2012.

[15] F. Bao, C.-C. Lee, and M.-S. Hwang, "Cryptanalysis and improvement on batch verifying multiple RSA digital signatures," *Applied Mathematics and Computation*, vol. 172, no. 2, pp. 1195–1200, 2006.

[16] Z. Zhang and J. Luo, "A data value classification and encryption mechanism based on metadata attributes," *Journal of Northwest University*, vol. 46, no. 2, pp. 188–194, 2016.

[17] T. Liu, Y. Liu, Y. Mao et al., "A dynamic secret-based encryption scheme for smart grid wireless communication," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1175–1182, 2014.

[18] M. A. Wei-Wei, "Research on security encryption for information acquisition under mobile Internet," *Electronic Design Engineering*, vol. 26, no. 23, 2018.

[19] S. Sedghi, J. Doumen, P. Hartel, and W. Jonker, "Towards an information theoretic analysis of searchable encryption," in *Information and Communications Security*, pp. 345–360, Springer, 2008.

[20] Y. Qin, Z. Wang, H. Wang, Q. Gong, and N. Zhou, "Robust information encryption diffractive-imaging-based scheme with special phase retrieval algorithm for a customized data container," *Optics and Lasers in Engineering*, vol. 105, pp. 118–124, 2018.

[21] L. Teng and H. Li, "CSDK: a chi-square distribution-Kernel method for image de-noising under the Internet of things big data environment," *International Journal of Distributed Sensor Networks*, vol. 15, no. 5, 2019.

[22] Y. Sun, S. Yin, H. Li, L. Teng, and S. Karim, "GPOGC: Gaussian pigeon-oriented graph clustering algorithm for social networks cluster," *IEEE Access*, vol. 7, pp. 99254–99262, 2019.

[23] X. Wang, S. Yin, H. Li, L. Teng, and S. Karim, "A modified homomorphic encryption method for multiple keywords retrieval," *International Journal of Network Security*, 2020.

[24] N. Sidaty, M. Viitanen, W. Hamidouche, J. Vanne, and O. Deforges, "Live demonstration: end-to-end real-time ROI-based encryption in HEVC videos," in *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*, p. 1, Florence, Italy, 2018.

[25] M. Hwang, E. Cahyadi, C. Yang, and S. Chiou, "An improvement of the remote authentication scheme for anonymous users using an elliptic curve cryptosystem," in *2018 IEEE 4th International Conference on Computer and Communications (ICCC)*, pp. 1872–1877, Chengdu, China, 2018.

[26] C. Yang, Y. Lin, and M. Hwang, "Downlink relay selection algorithm for amplify-and-forward cooperative communication systems," in *2013 Seventh International Conference on Complex, Intelligent, and Software Intensive Systems*, pp. 331–334, Taichung, Taiwan, 2013.

[27] L. Teng and H. Li, "A high-efficiency discrete logarithm-based multi-proxy blind signature scheme via elliptic curve and bilinear mapping," *International Journal of Network Security*, vol. 20, no. 6, pp. 1200–1205, 2018.

[28] J. Luo, Q. Dong, D. Huang, and M. Kang, "Attribute based encryption for information sharing on tactical mobile networks," in *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, pp. 1–9, Los Angeles, CA, USA, 2018.

[29] R. Yadav, W. Zhang, O. Kaiwartya, P. R. Singh, I. A. Elgendy, and Y.-C. Tian, "Adaptive energy-aware algorithms for minimizing energy consumption and SLA violation in cloud computing," *IEEE Access*, vol. 6, pp. 55923–55936, 2018.

[30] R. Yadav, W. Zhang, K. Li, C. Liu, M. Shafiq, and N. K. Karn, "An adaptive heuristic for managing energy consumption and overloaded hosts in a cloud data center," *Wireless Networks*, vol. 26, no. 3, pp. 1905–1919, 2020.

[31] A. U. Makarfi, R. Kharel, K. M. Rabie, O. Kaiwartya, and G. Nauryzbayev, "Physical layer security in vehicular communication networks in the presence of interference," in *2019 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, Waikoloa, HI, USA, 2019.

[32] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, X. Li, and R. Kharel, "Physical layer security in vehicular networks with reconfigurable intelligent surfaces," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, pp. 1–6, Antwerp, Belgium, 2020.

[33] A. A. A. Punitha and G. Indumathi, "Centralized cloud information accountability with bat key generation algorithm (CCIA-BKGA) framework in cloud computing environment," *Cluster Computing*, vol. 22, pp. 3153–3164, 2019.

[34] J. Li, L. Chen, Y. Lu, and Y. Zhang, "Anonymous certificate-based broadcast encryption with constant decryption cost," *Information Sciences*, vol. 454-455, pp. 110–127, 2018.

[35] B. Hiemenz and M. Kramer, "Dynamic searchable symmetric encryption for storing geospatial data in the cloud," *International Journal of Information Security*, vol. 18, no. 3, pp. 333–354, 2019.