Hindawi
Journal of Mathematics
Volume 2022, Article ID 7138173, 11 pages
https://doi.org/10.1155/2022/7138173

Research Article

Design of Updating Encryption Algorithm for Privacy Big Data Based on Consortium Blockchain Technology

Lei Liu,[1,2,3] **Xue Liu**,[3] **and Jiahua Wan**[3]

[1]*Institute of Intelligent Machines, Hefei Institutes of Physical Science, Chinese Academy of Sciences, Hefei 230031, China*
[2]*University of Science and Technology of China, Hefei 230026, China*
[3]*Anhui Xinhua University, Hefei 230088, China*

Correspondence should be addressed to Xue Liu; liuxue@axhu.edu.cn

Received 24 August 2022; Revised 12 September 2022; Accepted 20 September 2022; Published 11 October 2022

Academic Editor: Shenggang Li

The existing privacy big data encryption algorithm cannot achieve real-time update of big data and repeat more big data, resulting in low attack resistance and more malicious attack data. An updating encryption algorithm for privacy big data based on consortium blockchain technology is proposed in this paper. The redundancy of privacy big data is obtained, the deduplication technology is designed on this basis, and the big data preprocessing is completed. The source coding sequence of privacy big data is obtained, the security of network route query and identity is verified, and the update and extraction of user data access authority are realized. The data structure of encrypted block is generated by using consortium blockchain technology and updating homomorphic encryption technology to realize the updating encryption algorithm of privacy big data. Experimental results show that the proposed algorithm improves the ability of resisting attacks and the amount of malicious data intercepted. The encryption complexity is lower, the time consumption is shorter, and the error of privacy large data encryption is smaller.

1. Introduction

Blockchain realizes the distributed storage and decentralization of data through chain structure and P2P network. Use the consensus mechanism to make the nodes in the network reach an agreement and ensure the consistency of data. Adopt cryptography technology to ensure the integrity, traceability, and immutability of information in the block. It also supports users to create flexible smart contracts, which greatly expands the application of blockchain. The current economic development strategy makes big data from open to open development and becomes a new stage of information development. Information will be open to processing through opening big data, and in-depth understanding of the development of various industries will be achieved. Enhancing data value through the use of privacy big data enables effective participation of the general public in big data governance [1]. However, with the current development of open big data, the current open data platform cannot guarantee the security of open big data due to its short development time, causing personal private data and key data significant security threats [2]. Therefore, the largest obstacle to opening big data is how to ensure the security of big data, and the existing encryption algorithm is unsuitable for complex data processing. And encryption algorithms are an important part of blockchain. Improving the encryption algorithm in the blockchain is the most important link in improving the performance of the blockchain.

Reference [3] designs an encryption algorithm based on cloud computing technology and multichaotic mapping algorithm. In accordance with piecewise linear chaotic mapping, the data to be encrypted are transformed into chaotic sequence, where the data index matrix is generated to replace the plaintext big data. For the data after cyclic shift processing, logistic chaotic sequence is used to generate the encrypted results. However, the encryption process of this method has more redundant data. Reference [4] deeply processes data packets and divides them into two important categories in accordance with privacy weight. The encryption time of each category packet is studied, the weight

calculation results are obtained, and the weight calculation results are sorted in descending order. The first packet is encrypted and transmitted because each packet has corresponding transmission paths. Simultaneous interpretation of the remaining time of the channel after transmission is completed, and the remaining data packets are allocated to different transmission paths to achieve the overall encryption of the data. However, this data processing method takes extremely long to encrypt. Reference [5] constructs a bloom filter redundancy elimination algorithm based on data redundancy elimination technology. The similarity between the data to be processed is obtained through the Hamming distance calculation results. The elliptic encryption algorithm is used to process the data after the redundant data are removed. The big data encryption model is designed through the combination of symmetric and asymmetric encryption algorithms. The verification shows that the encryption security of this method is poor in practical application. In reference [6–8], scholars describe how the development of sustainable products and processes is critical to the survival of manufacturers in today's competitive markets and in the industrial 4.0 era. The activities of manufacturers and their supply chain partners shall be consistent with the sustainable development goals. As a result of globalization, outsourcing, and offshoring, manufacturers face many obstacles and challenges in implementing sustainable practices throughout their supply chains. Blockchain technology has the potential to address sustainability challenges. The study explains the application of blockchain technology in sustainable manufacturing and the potential contribution of blockchain technology to the economic, environmental, and social performance of manufacturers and their supply chains

Data encryption is becoming more and more important in the alliance chain. With the more and more extensive use of the alliance chain and the increasing amount of data, how to encrypt big data quickly becomes particularly important. On the basis of the above data encryption methods and considering the shortcomings of traditional encryption methods, a new refreshable encryption algorithm is designed. Private big data are pretreated by data deduplication, and sensitive big data are encrypted by association chain technology.

2. Privacy Big Data Update Encryption Algorithm Based on Alliance Chain Technology

The transaction layer in the blockchain records the entire process through which a user's data is generated, verified, stored, and used. In order to protect the privacy of user data in the transaction layer, the technology that can be used mainly includes data encryption technology and data distortion technology. An updating encryption algorithm for privacy big data based on consortium blockchain technology is proposed in this paper. Firstly, the redundancy of privacy big data is obtained, and on this basis, the deduplication technology is designed to complete the preprocessing of big data. Then, the source coding sequence of private big data is obtained to verify the security of network routing query and identity, and the update and extraction of user data access rights are realized. Finally, the joint chain technology and update homomorphic encryption technology are used to generate the data structure of encryption block, and the update encryption algorithm of privacy big data is realized.

2.1. Privacy Big Data Preprocessing. In the process of big data encryption, adding deduplication technology can effectively reduce the computational complexity of the encryption algorithm. Data deduplication technology is designed on the basis of an in-depth analysis of privacy big data to obtain the redundancy of the data itself. The displayed data objects are unique, and the other data samples with high similarity are replaced by the unique data objects by processing the duplicated data in big data. The data dimension can be reduced, and the data storage space can be reduced effectively by eliminating redundant data in the file by preprocessing technology. The data storage space is optimized through data deduplication technology, effectively reducing the workload of encryption processing and improving the efficiency of large data update encryption. Because more duplicated data will take up more data storage space, data shrinkage can make data take up less space, and the direct benefit of data shrinkage is to store the same data with less space; so, the calculation of data shrinkage rate is very important in data processing.

After deduplication, the data reduction rate S is calculated as follows:

$$S = \frac{B}{B'}, \tag{1}$$

where B represents the number of bytes before deduplication, and B' represents the number of bytes after redundancy processing. The privacy of large data type partitioning strategy and partitioning data block size affect the results through the in-depth analysis of the data reduction rate.

In the process of data reduction rate calculation, the duplicate data between data blocks are included, but the influence of data overhead is ignored. Therefore, in the design process of the data deduplication technology, relying on the metadata overhead, the data reduction rate calculation formula needs to be modified to obtain the calculation process of Formula (2).

$$S = \frac{S}{1 + \chi}, \tag{2}$$

where χ represents the cost of metadata size, and its calculation formula is as follows:

$$\chi = \frac{Y_{\text{MetadataSize}}}{Y_{\text{AverageChunkSize}}}, \tag{3}$$

where $Y_{\text{MetadataSize}}$ represents the metadata size, and $Y_{\text{AverageChunkSize}}$ represents the average data block size. On

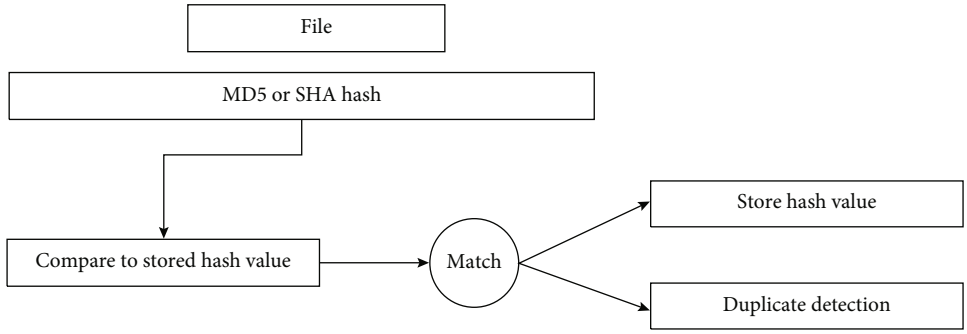


Figure 1: Complete file detection framework.

the basis of the above deduplication technology, this paper adopts the full file detection technology to analyze the same data contained in the data set and annotate the same data monitored. In accordance with the data detection results, data types are divided in a fine-grained manner, and the data belonging to redundant data classification are removed [9].

On the basis of the full file detection technique shown in Figure 1, each file is chunked to find duplicate data from the dataset in accordance with the granularity of the individual data block. In the actual data detection process, the hash value of the private big data is compared with the hash value stored in advance in accordance with the calculation result. When the two hash values are consistent, the file is stored directly; otherwise, a deduplication operation is required. After the big data privacy preprocessing is completed, it provides data support for encryption processing.

2.2. Big Data Bit Sequence Preprocessing. The most important component of privacy big data is the bit sequence, which can greatly improve the concealment of users' location after preprocessing, so that attackers cannot obtain privacy big data. If the two bit sequences of privacy big data are listed as $a_0, a_1, a_2, \cdots, a_n$ and $b_0, b_1, b_2, \cdots, b_n$, the scheduling parameter is set to p, and the random distribution models M_1 and M_2 are obtained by adjusting and controlling the binary sequence of n dimension parameter p, where the expression of the encoding sequence of information source of privacy big data is [10].

$$x = \{x_i, i = 1, 2, \cdots, N | x_i \in X\}, \tag{4}$$

where X represents the binary vector quantization function of privacy big data of any information source, and the information source belongs to the position sequence of information source coding.

On the basis of adaptive piecewise linear equilibrium, position data feature $e : M_1 \times M_1 \longrightarrow M_2$ is mined, and most character sequences are encrypted by ciphertext. All the secret key $p_0, p_1, \cdots, p_{l-1}$ in the big data bit sequence is obtained by using ciphertext sequence. In each encryption cycle, ciphertext sequence is reconstructed by means of three retransmissions, and then the mapping relation of anonymity of the big data is obtained.

In accordance with this scheme, the parameter secret key $C = (C_1, C_2, C_3, C_4, C_5)$ is obtained, and any code element in the privacy big data link layer is selected. $h \in M_1/\{1_{M_1}\}$, $H_0 \in M_2/\{1_{M_2}\}$, and ξ_1 and ξ_2 belong to the position sequence Z_p^* of information source coding. The threshold value can be obtained by mapping them into the code element $\{1_{M_2}\}$ and $\{1_{M_1}\}$, and the expression is as follows:

$$P = 2[1 - C(x)] \cdot w, \tag{5}$$

where w represents the original link location.

When the threshold is greater than or equal to 0.01, the group function of privacy large data is a random distribution.

2.3. User and Network Routing Inquiry and Identity Authentication. In the specific application process, the user's identity information and virtual currency transaction information are easily obtained by attackers at the network layer, transaction layer, and application layer, and it is easy for others to illegally use the user's data. This chapter uses user and network routing query and identity authentication to verify the security of network routing query and identity identification. Pseudorandom number r_X is generated by user X of pseudorandom function generator and transmitted to network route Y as big data access request, and a new session cycle is started. When the r_X transmitted by user X is received by the network route Y, the network route Y generates a corresponding pseudorandom number r_Y and selects any number $c \in Z_q$, where q represents a large prime number, which is obtained by calculating f_i and h_i as follows:

$$f_i = h^{c^{i-1}} (i = \{1, 2, \cdots, n\} \in Z). \tag{6}$$

Set $F = (q, f, h, F, F', e, H)$ to represent a matching group, where $F = \langle f \rangle = \langle h \rangle$, F', to the multiplicative group of q and $H(\cdot)$ to a collision-free hash function. The principal public key mpk and the principal private key msk are generated by network routing Y, which can be represented as follows:

$$\begin{cases} \text{mpk} = (F), \\ \text{msk} = (c, f). \end{cases} \tag{7}$$

Primary public keys mpk and r_Y, which are routed by the network, are transmitted to user X as acknowledgement responses.

When the network route Y transmitted $r_Y \| \text{mpk}$ is received by user X, the arbitrary value k is selected, and the pseudonym PID_X is extracted. User X performs operations by using the Chebyshev polynomial function $\tau_k(\cdot)$ to obtain the values C_X and D_X.

$$\begin{cases} C_X = \tau_k(R) \bmod q, \\ D_X = \tau_k(Q) \bmod q. \end{cases} \tag{8}$$

Temporary identity identifier TID_X is obtained by user X continuing the operation to [11]

$$\text{TID}_X = \text{CD}_X \in H(D_X \| r_X). \tag{9}$$

Data $C_X \| \text{TID}_X \| H_X$ are transmitted from user X to network route Y, and the network route conducts operation with $\tau_x(\cdot)$ to obtain the numerical value TID'_X.

$$\text{TID}'_X = C_X \in \psi\left(D'_X \| r_X\right). \tag{10}$$

Network routing Y compares the numeric value H^{ℓ}_X obtained from the second operation with the received value H_X. If the two values are the same, user X can be identified as legal, and the access control protocol can continue; otherwise, the access control protocol can be terminated.

2.4. Big Data Access Permissions Can Be Updated and Extracted. In order to extract the updated access rights of big data, it is necessary to select any data combination as the authorized big data and set the corresponding users of the authorized big data set as the sample users. Network routing Y selects any number $\sigma \in \{0,1\}^*$ and realizes the update extraction of user's data access rights policy [12, 13]. The user has access to the default authorization big data S_X and can meet the control requirements of updatable access policy O_X. Network routing is based on O_X, implemented by network routing Y to numeric $\{M_0, M_1, \{M_{2i}\}, M_3, M_4\}$, generating ciphertext $A'_X = (M_0, M_1, \{M_{2i}\}, M_3, M_4)$ and transmitting ciphertext to user X. The numerical combinations that are performed are

$$M_0 = \psi\left(S_X \| \text{TID}'_X \| \sigma\right), \tag{11}$$

$$M_1 = \left(h^{\rho(c,O_X)}\right)^{M_0}, \tag{12}$$

$$M_{2i} = (f_i)^{M_0}, (i = \{1, \cdots, n\}), \tag{13}$$

$$M_3 = \psi\left(e(f,h)^{M_0}\right) \oplus \sigma, \tag{14}$$

$$M_4 = \psi(r_X \| \sigma) \oplus S_X. \tag{15}$$

The user calculates $\{N_{X1}, N_{X2}, N_{X3}\}$ set of value, which can be expressed as

$$\begin{cases} N_{X1} = e(M_1, M_2, M_3, M_4), \\ N_{X2} = e\left(\prod_{i=1}^{n} (M_{2i})^{f_i{}'}\right), \\ N_{X3} = \left(f^{\beta+1/\rho(c,C_X)}, M_1, M_2, M_3, M_4\right). \end{cases} \tag{16}$$

In polynomial (16), the coefficients of x^i in polynomial $\rho(x, O_X)$ are expressed in terms of f'_i, and the coefficients of x^i in polynomial $\rho(x, L_X)$ are expressed in terms of f'_{Xi}. The algebraic relation to which $e(f,h)$ must conform can be expressed as

$$e(f,h) = \left(\frac{N_{X3}}{N_{X1}N_{X2}}\right). \tag{17}$$

After decrypting the numeric value κ again, the user obtains the big data S_X, which is authorized by the numeric value by default. The two can be represented as

$$\begin{cases} \sigma^{\ell} = M_3 \oplus \psi(e(f,h)), \\ S_X = M_4 \oplus \psi(r_X \| \kappa). \end{cases} \tag{18}$$

2.5. Update Encryption of Privacy Big Data Based on Federation Chain Technology. Aiming at the big data access right extracted from the above calculation, this paper adopts the consortium blockchain technology [14, 15] and the updated homomorphic encryption technology [16] to generate the encrypted block data structure. Compared with the conventional federated chain, the updated homomorphic encryption is used to protect the sensitive data more effectively. On the basis of the private association chain formed by the data structure of updatable and encrypted blocks, the sensitive data in the private big data are encrypted to form the ciphertext information and stored in the block. In accordance with the above sensitive big data recognition technology, the open big data are divided into sensitive data and public data, and only updating homomorphic encryption is needed.

The homomorphic Paillie algorithm is selected to encrypt the image. The steps are as follows. Two large prime numbers are randomly selected, and the minimum common multiple N between them is calculated. An integer g is selected, so that $g \bmod N^2 = 1$, and N, g represents the public and private keys generated by the big data encryption process, respectively. An integer is selected randomly, so that the sensitive data identified above belong to the integer, the sensitive data are encrypted by the public key, and the corresponding ciphertext c is obtained.

The sensitive and nonsensitive data are aggregated to form the data set g, and a corresponding private key is allocated to each g signature by using the consortium blockchain technology. For the data with corresponding signatures, the hash value of the data is calculated by hashing, and the results are placed in the blocks of the federated chain [17]. Considering the additive homomorphism of the Paillie encryption algorithm, this paper selects an open big

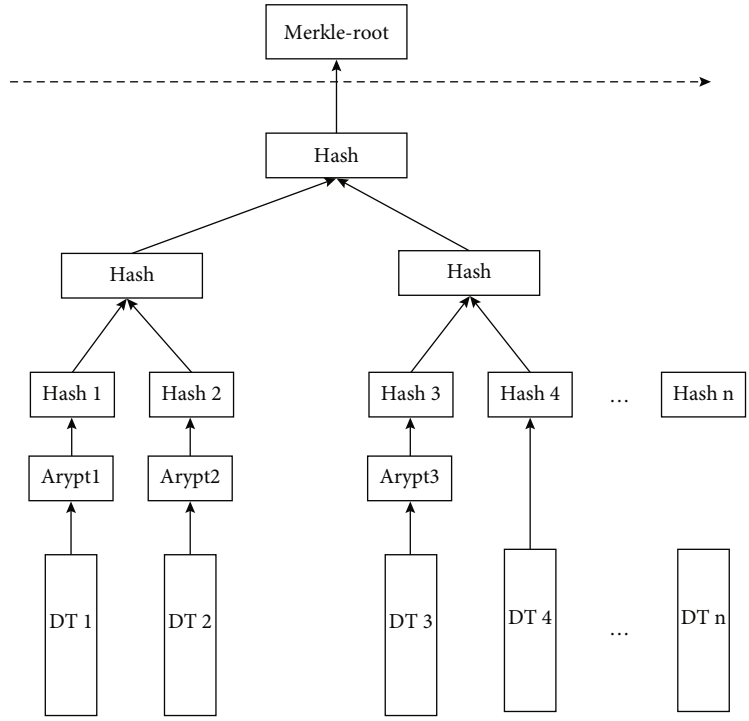


Figure 2: Block data structure based on homomorphic encryption.

data for analysis and finds that the big data contain two access records. Encryption processing is conducted for each access record, and the following updated encryption formula is obtained.

$$\begin{cases} y_1 = E(v_1, r_1), \\ y_2 = E(v_2, r_2), \\ y_1 \cdot y_2 = E(v_1, r_1) \cdot E(v_2, r_2), \end{cases} \tag{19}$$

where y_1 represents the first access to the encryption results, and y_2 represents the updated access encryption results. v_1 , v_2 represent the two access times, r_1, r_2 are the access log cipher, and g is the public key, N is the private key, and E denotes the arbitrary operation. The encrypted cipher text of open large data can be obtained without publishing the records of two visits through the above encryption processing.

The decryption of ciphertext needs to be based on clear text. The decryption formula is

$$g = D(y_1 \cdot y_2) = \left[\frac{(y \bmod N^2)}{(\bmod N^2)} \right] \bmod N. \tag{20}$$

After processing in accordance with the updatable homomorphic encryption technology, the data results of the new alliance chain are obtained, and the generated structure is shown in Figure 2.

In the block data structure shown in Figure 2, the open big data are partitioned, and the private data are selected to update homomorphic encryption to form hash data DT. The large data can be updated and encrypted by the encrypted block data structure formed by the above operation.

Table 1: Computer configuration parameters required for the experiment.

Name	Frequency	Memory	Hard disk
Cloud2	3.0 G	512 MB	80 G
Cloud3	3.0 G	512 MB	80 G
Cloud4	3.0 G	512 MB	80 G
Node1	3.0 G	3 G	150 G
Node2	3.0 G	3 G	150 G
Node3	3.0 G	3 G	150 G

3. Experiments and Results

The complexity of encryption, encryption efficiency, and key sensitivity is tested on the Hadoop platform of a company's information security transmission system to verify the overall effectiveness of the proposed algorithm.

3.1. Experiment Platform. The platform selected for the experiment of big data encryption algorithm is laboratory Hadoop, which mainly includes six computers. In accordance with the basic composition requirements of Hadoop platform, one of the computers is selected as the server to record name node and complete real-time adjustment of experimental data. The other computers are used as the main experimental tools to play the role of node computing and storage. Considering the actual application environment, the configuration of the five computers acting as

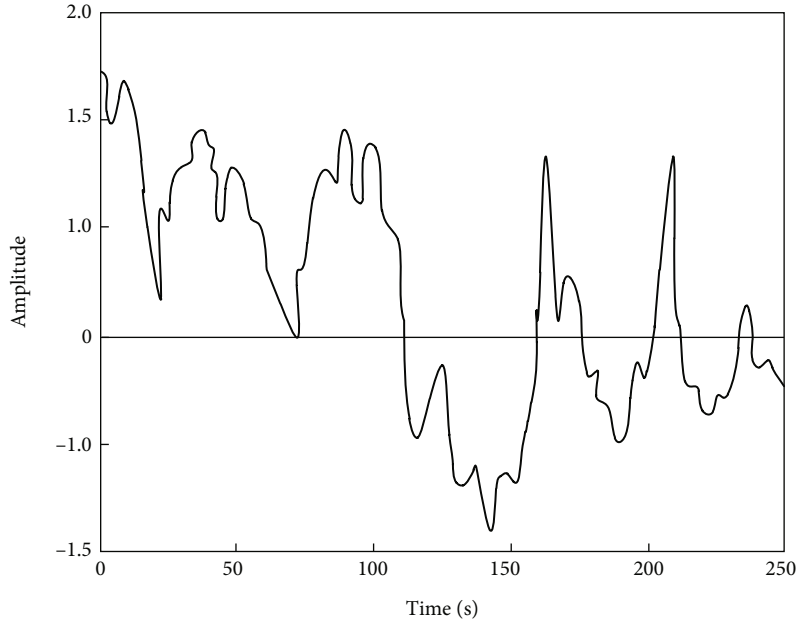


Figure 3: Amplitude variation of privacy data to be encrypted.

experimental tools is relatively different to enhance the authenticity of the experimental environment. In the construction of the experimental platform, computer configuration parameters are shown in Table 1.

In accordance with the computer configuration parameters shown in Table 1, the experimental platform contains three computers with strong computing and storage levels. Referring to the practical application environment, a computer with strong performance is selected to act as the computing and storage node, so that the experimental environment can meet the requirements of cryptographic algorithm. In addition to the above hardware requirements, the design of the experimental platform has higher requirements for the software needed for the experiment. In accordance with the above requirements, the experimental platform can ensure the stability of the experiment and more intuitively show the performance of the privacy big data update encryption algorithm.

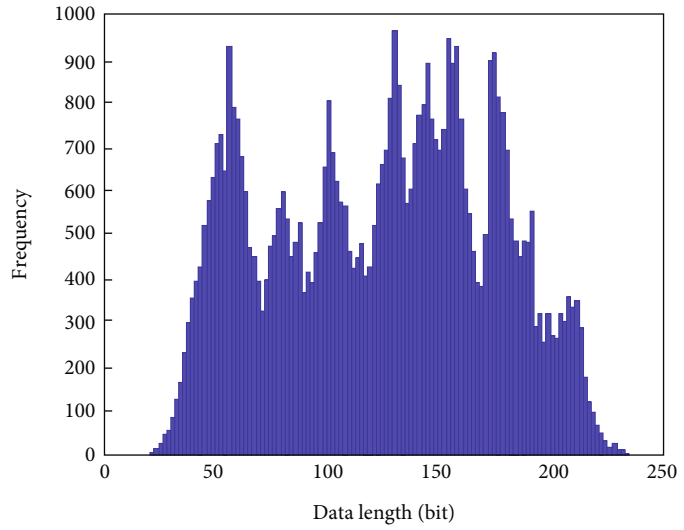
3.2. Encryption Function Test. In the experiment, a data file with the size of 159,874 KB is used as the experimental sample in the updating encryption algorithm of big data based on the chain. Considering the large amount of privacy data, many large data files will be placed in the open data platform when sharing the data. Therefore, the application process of the updating encryption algorithm for large data needs to meet the requirement of large file encryption. Thus, when we test the encryption function of the design method in this paper, we choose large files as experimental data to obtain more accurate application results. In the process of data encrypting and decrypting, the amplitude change of private data to be encrypted is formed in accordance with the length of sample and the private data to be encrypted, as shown in Figure 3.

The amplitude change of privacy data shown in Figure 3 is obtained when the sample block length is set to 120 bit, and the data encryption function test is conducted on this basis. On the basis of the above experimental data, the design method in this paper is used to test the updatable encryption.

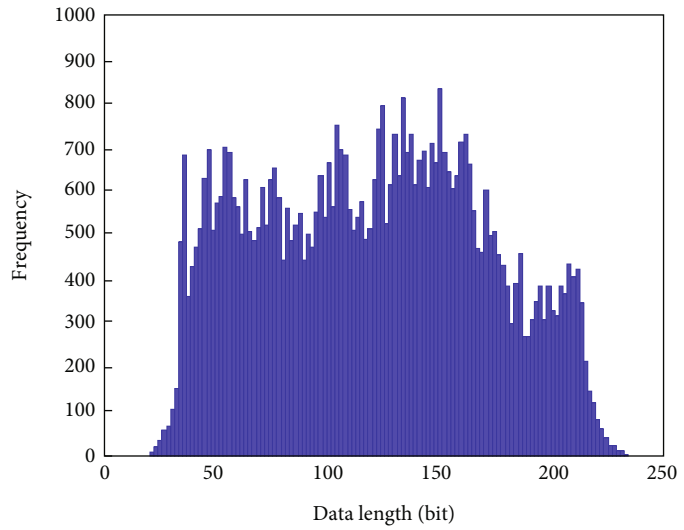
When privacy big data is invaded or at risk of theft, the intruder will compare the ciphertext data statistics with the plaintext statistics, so that the breaker can obtain the transformation rule between the plaintext and ciphertext based on this. The randomness of ciphertext statistics is ensured to improve data encryption. In the experimental process, the same experimental data are encrypted by using the big data encryption algorithm based on weight calculation proposed in reference [4] and the big data encryption algorithm based on bloom filter redundancy proposed in reference [5]. The processing results of the three algorithms are described in terms of histogram. The comparison results of big data encryption effects are shown in Figure 4.

The more uniform the histogram distribution results, the better the data encryption effect. In accordance with the histogram comparison results shown in Figure 4, compared with the original image, the histogram distribution of the big data encryption algorithm based on weight calculation proposed in reference [4] and the big data encryption algorithm based on bloom filter redundancy proposed in reference [5] changes toward homogenization but cannot meet the encryption requirements. The histogram obtained by the proposed encryption algorithm is extremely uniform, thereby improving the difficulty of the attacker's ciphertext decoding and effectively enhancing the attack resistance of the algorithm.

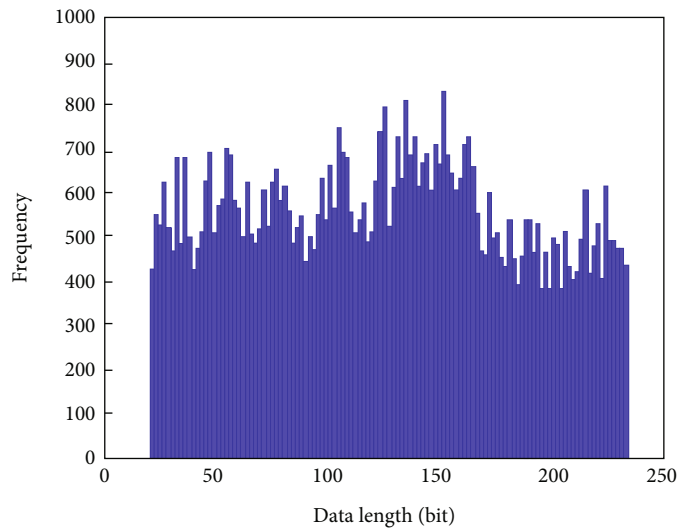
3.3. Encryption Complexity. The shorter the key data, the lower the encryption complexity. The data in Figure 5 show that the security of two other algorithms is higher. The key length of bloom filter away redundant big data encryption algorithm is higher than 7200. The key length of the



(a) Raw data

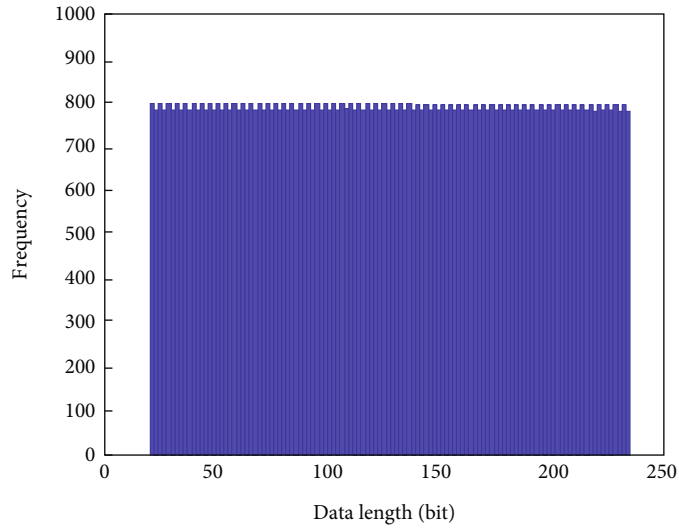


(b) Big data encryption algorithm based on weight calculation



(c) Big data encryption algorithm based on bloom filter redundancy elimination

Figure 4: Continued.



(d) Scalable encryption algorithm for privacy big data based on alliance chain technology

Figure 4: Comparison of big data encryption effects.

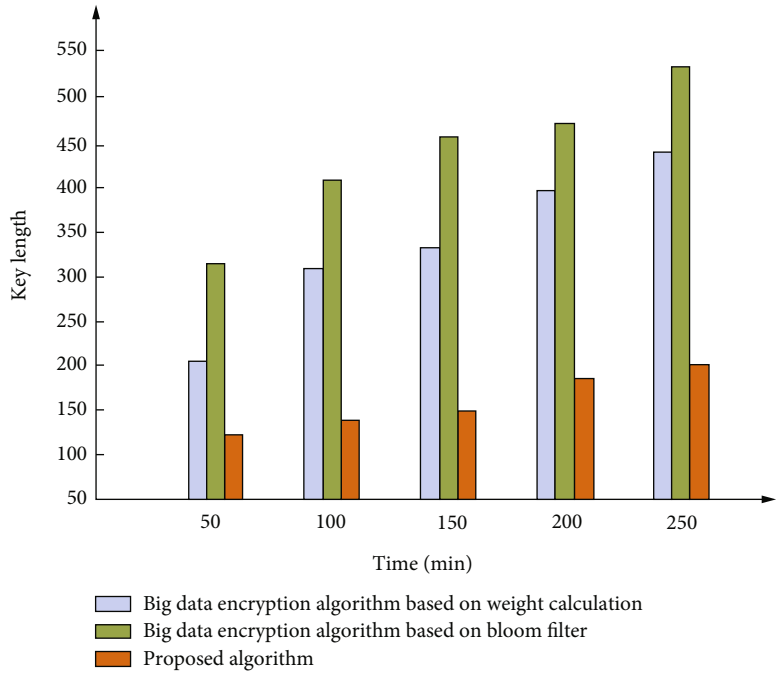


Figure 5: Encryption complexity of different algorithms.

proposed algorithm under the same security level is the shortest, and its grade is 300 regardless of its length. The proposed algorithm uses the revocable encryption algorithm and the federation chain encryption algorithm to form a hybrid encryption algorithm to encrypt the private big data, greatly improving the encryption performance and reducing the encryption complexity.

3.4. Encryption Efficiency. Comparing the time spent in different stages of the encryption process of the three algorithms, Figure 6 shows that the time spent in each stage of the algorithm is the lowest, and all the time spent in all stages are added together to form the time spent in encryption. The time spent on the encryption of the algorithm is only 3.56 s, the time spent on the big data encryption algorithm based on weight calculation is 7.58 s, and the time spent in the encryption of the big data encryption algorithm based on bloom filter is more than 10 S, proving that the time spent on the encryption of the proposed algorithm is the best. This condition is because the double-layer encryption strategy is adopted in the encryption of the privacy big data information to obtain double keys to encrypt, accelerate the encryption, reduce the encryption time, and improve the encryption efficiency.

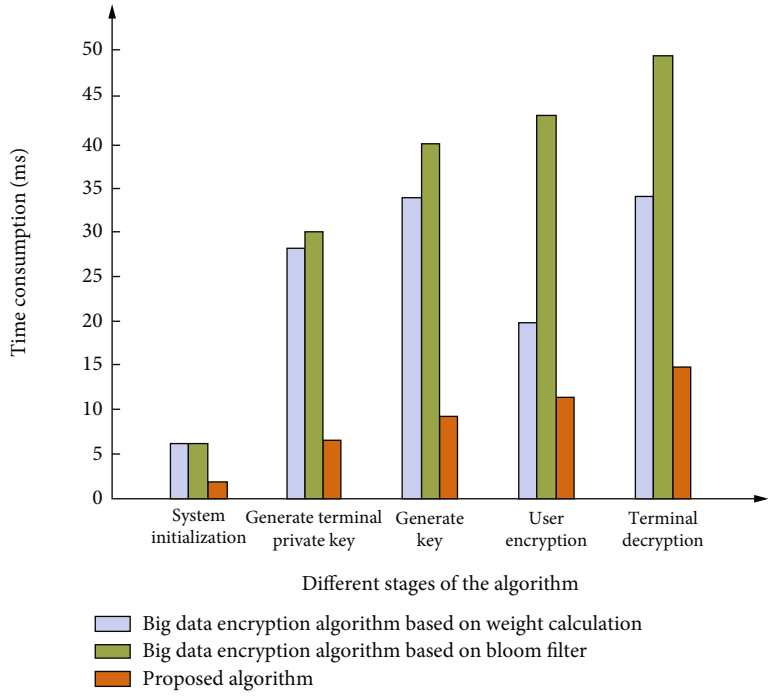


Figure 6: Time consumption of the three algorithms at different stages.

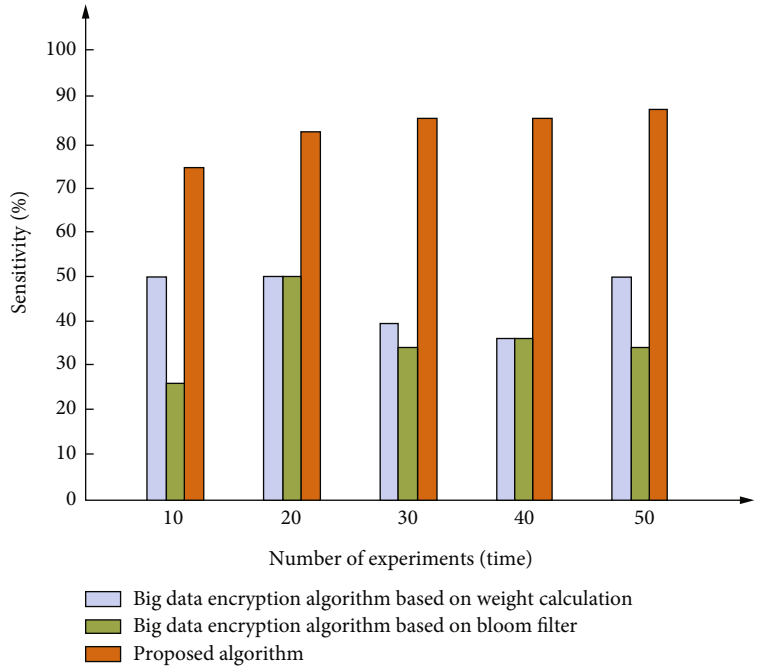


Figure 7: Comparative test of key sensitivity of different algorithms.

3.5. Sensitivity of the Encryption Algorithm. The symmetric encryption algorithm and public key encryption algorithm of the encryption algorithm constitute the plaintext sensitivity. Therefore, if the plaintext changes, then the ciphertext data change accordingly. The greater the change, the more sensitive the algorithm. As shown in Figure 7, the sensitivity of the big data encryption algorithm based on bloom filter redundancy proposed by the algorithm is compared with the proposed algorithm and the big data encryption algorithm based on weight calculation proposed in references [4, 5] through many experiments. The sensitivity of the proposed algorithm remains more than 50% after many iterations, whereas the sensitivity of the big data encryption algorithm based on weight calculation and the big data encryption algorithm based on bloom filter redundancy is extremely low. The proposed algorithm first designs a

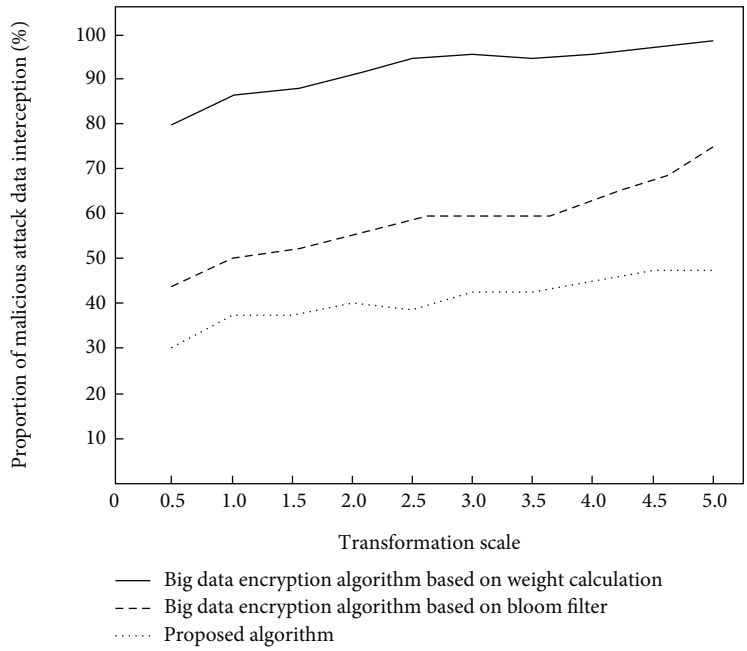


Figure 8: Malicious attack data interception volume of different algorithms.

revocable encryption algorithm with key encryption key and then encrypts private big data, so as to strengthen the flexibility of private big data encryption algorithm and improve the sensitivity of the algorithm.

3.6. Malicious Attack Data Interception Test. As shown in Figure 8, with the increase in transformation scale, the interception volume of malicious attack data of the three methods increases, but the interception volume of big data encryption algorithm based on bloom filter redundancy elimination does not increase. The interception volume increases by less than 10%, and the interception volume of big data encryption algorithm based on weight calculation increases significantly, but the maximum interception volume is only 70%. This value is still lower than the interception amount of the proposed algorithm. This is because the algorithm encrypts the user's location anonymously and sets up encrypted defenses in advance before updating the private big data, which greatly ensures the security of the database and improves the amount of data intercepted by malicious attacks.

3.7. Data Encryption Error Test. As shown in Figure 9, when the data set is 3, the error of the algorithm in reference [4] is the smallest. The error of the big data encryption algorithm based on weight calculation is approximately 5.0. When the data set is 5, the error of the big data encryption algorithm based on bloom filter redundancy is the smallest. The error of the big data encryption algorithm based on bloom filter redundancy is approximately 6.0. The error of the proposed method is approximately 2.0. This condition is because the proposed method conducts data encryption search after bit sequence preprocessing for privacy big data in advance hides most of the user's privacy in advance, encrypts the user's search content, greatly improves the encryption accuracy, and reduces the encryption error.

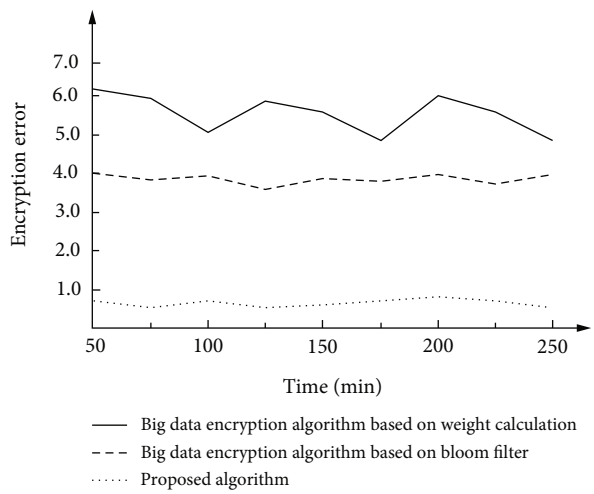


Figure 9: Comparative test of encryption error of different algorithms.

4. Conclusion

A privacy big data updatable encryption algorithm based on alliance chain technology is proposed to solve the problem that the attack resistance of traditional privacy big data encryption algorithms is low, and the amount of malicious attack data is still large. Data deduplication technology is designed to obtain the information source coding sequence of privacy big data and realize the updatable extraction of users' data access right policy. Alliance chain technology is introduced to realize the updatable encryption algorithm of

private big data and optimize the encryption effect of big data. The experimental results show that the designed algorithm is effective, has ideal attack resistance, has a large amount of malicious attack data interception, has low encryption complexity, takes less time, and has good applicability. Experiments show that this method effectively improves the security of private big data.

Data Availability

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

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was financially supported by the Universities Blockchain Technology Innovation Action Plan and Fund (2020jyxm0789 and 2020qk121, respectively).

References

[1] H. Chergui and C. Verikoukis, "Big data for 5G intelligent network slicing management," *IEEE Network*, vol. 34, no. 4, pp. 56–61, 2020.

[2] K. Sudhakar, M. A. H. Farquad, and G. Narshimha, "Effective convolution method for privacy preserving in cloud over big data using map reduce framework," *IET Software*, vol. 13, no. 3, pp. 187–194, 2019.

[3] J. L. Tian, "Research on hybrid chaotic encryption algorithm based on cloud computing," *Application of Electronic Technique*, vol. 46, no. 10, pp. 79–82, 87, 2020.

[4] M. Yin, "Automatic encryption simulation of private data in online bidding system," *Computer Simulation*, vol. 37, no. 5, pp. 128–131, 212, 2020.

[5] P. Han, C. Liu, J. Wang, S. Duan, H. Pan, and B. Fang, "Research on data encryption system and technology for cloud storage," *Journal on Communications*, vol. 41, no. 8, pp. 55–65, 2020.

[6] A. Khanfar, M. Iranmanesh, M. Ghobakhloo, M. G. Senali, and M. Fathi, "Applications of blockchain technology in sustainable manufacturing and supply chain management: a systematic review," *Sustainability*, vol. 13, no. 14, p. 7870, 2021.

[7] Y. Zhou, H. Liu, J. Cao, and S. Li, "Composite learning fuzzy synchronization for incommensurate fractional-order chaotic systems with time-varying delays," *International Journal of Adaptive Control and Signal Processing*, vol. 33, no. 12, pp. 1739–1758, 2019.

[8] Y. Zhou, H. Wang, and H. Liu, "Generalized function projective synchronization of incommensurate fractional-order chaotic systems with inputs saturation," *International Journal of Fuzzy Systems*, vol. 21, no. 3, pp. 823–836, 2019.

[9] Y. Cui, "Intelligent recommendation system based on mathematical modeling in personalized data mining," *Mathematical Problems in Engineering*, vol. 2021, no. 3, Article ID 6672036, 11 pages, 2021.

[10] X. Shi, F. Lv, D. Seng, B. Xing, and B. Chen, "Visual exploration of mobility dynamics based on multisource mobility datasets and POI information," *Journal of Visualization*, vol. 22, no. 6, pp. 1209–1223, 2019.

[11] C. Meshram, C. C. Lee, S. G. Meshram, and M. K. Khan, "An identity-based encryption technique using subtree for fuzzy user data sharing under cloud computing environment," *Soft Computing*, vol. 23, no. 24, pp. 13127–13138, 2019.

[12] K. A. Meerja, P. V. Naidu, and S. R. K. Kalva, "Price versus performance of big data analysis for cloud based Internet of Things networks," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 1078–1094, 2019.

[13] Z. Zhao, C. Feng, H. H. Yang, and X. Luo, "Federated-learning-enabled intelligent fog radio access networks: fundamental theory, key techniques, and future trends," *IEEE Wireless Communications*, vol. 27, no. 2, pp. 22–28, 2020.

[14] D. Fu, S. Hu, L. Zhang, S. He, and J. Qiu, "An intelligent cloud computing of trunk logistics alliance based on blockchain and big data," *The Journal of Supercomputing*, vol. 77, no. 12, pp. 13863–13878, 2021.

[15] S. Huang, G. Wang, Y. Yan, and X. Fang, "Blockchain-based data management for digital twin of product," *Journal of Manufacturing Systems*, vol. 54, pp. 361–371, 2020.

[16] M. S. Rahman, I. Khalil, M. Atiquzzaman, and X. Yi, "Towards privacy preserving AI based composition framework in edge networks using fully homomorphic encryption," *Engineering Applications of Artificial Intelligence*, vol. 94, article 103737, 2020.

[17] S. Garg, R. Singh, M. S. Obaidat, V. K. Bhalla, and B. Sharma, "Statistical vertical reduction-based data abridging technique for big network traffic dataset," *International Journal of Communication Systems*, vol. 33, no. 4, pp. e4249.1–e4249.13, 2020.