Hindawi
Journal of Sensors
Volume 2023, Article ID 9836943, 1 page
https://doi.org/10.1155/2023/9836943

Retraction

Retracted: Mathematical Modeling Analysis of Data Attribute Encryption for Robot

Journal of Sensors

Received 22 August 2023; Accepted 22 August 2023; Published 23 August 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] J. Sun, J. Yan, and D. Yang, "Mathematical Modeling Analysis of Data Attribute Encryption for Robot," *Journal of Sensors*, vol. 2022, Article ID 3976806, 8 pages, 2022.

Hindawi
Journal of Sensors
Volume 2022, Article ID 3976806, 8 pages
https://doi.org/10.1155/2022/3976806

Research Article

Mathematical Modeling Analysis of Data Attribute Encryption for Robot

Jingyi Sun,[1] **Jie Yan**,[2] **and Dingyi Yang**[2]

[1]*Department of Basic Education and Research, Changchun Finance College, Changchun, Jilin 130028, China*
[2]*School of Information Technology, Changchun Finance College, Changchun, Jilin 130028, China*

Correspondence should be addressed to Jingyi Sun; 1333307202@post.usts.edu.cn

Received 24 May 2022; Revised 25 June 2022; Accepted 4 July 2022; Published 23 July 2022

Academic Editor: Haibin Lv

Encrypting data based on the data attributes of robots is one of the effective methods to control access users in the data outsourcing environment. Therefore, a mathematical modeling method of robot data attribute encryption based on data redundancy elimination technology is proposed. The encryption algorithm structure is analyzed based on the Bloom filter. The Hamming distance is used to calculate the similarity of big data by the Bloom filter. Finally, a big data ellipse encryption algorithm is designed according to the calculation results. The results show that during the whole experiment, the approximate fluctuation range is 0.08%~0.14%, which is not only high but also has a large fluctuation range. In contrast, the probability of occurrence of redundant data is less than 0.05% under different byte rates of redundant data, which is far lower than the two traditional methods, indicating that the application performance of the proposed method is good.

1. Introduction

The mathematical modeling of big data attribute encryption uses mathematical methods to solve the problem of data encryption. Data encryption based on big data attributes is one of the effective methods to control data access users in the data outsourcing environment, but in the calculation process, it is impossible to realize the parallel application of multiple encryption methods. If the method is constantly updated, it will affect the execution efficiency of the overall algorithm and increase the time overhead [1]. In order to solve this problem, experts in relevant fields have obtained some good research results. According to the above situation, in the case of cloud computing data outsourcing environment, researchers propose a new method to expand data access and improve the security performance of encryption algorithm as a whole. For big data in multiauthority cloud, combined with improved attribute encryption, they propose a flexible and secure access control model, design a new policy update process based on improved proxy reencryption, and formulate an efficient policy update scheme [2, 3]. However, this method has the problem of more redundant data in the process of big data encryption. Other scholars have proposed a full homomorphic encryption method of multisource information resources in cloud computing environment with short public key, adding a set of homomorphic encryption of perceptual resources with the same remainder pair, extracting the real resources from the ciphertext data after additive fusion, then using the Chinese remainder theorem to verify the integrity of resources, and finally fusing the new security parameters into the integrity verification parameters. After linear conversion, the number of public key elements is reduced and the size of public key is improved [4, 5]. This method still has the problem that the encryption algorithm takes a long time. To solve the problems of the above traditional methods, we offer a mathematical modeling method for encrypting large data properties based on information resource technology. The structure of the encryption algorithm is analyzed based on the Bloom filter. Use the Hamming space to calculate the similarity of large data through a Bloom filter. Finally, the big data elliptic encryption

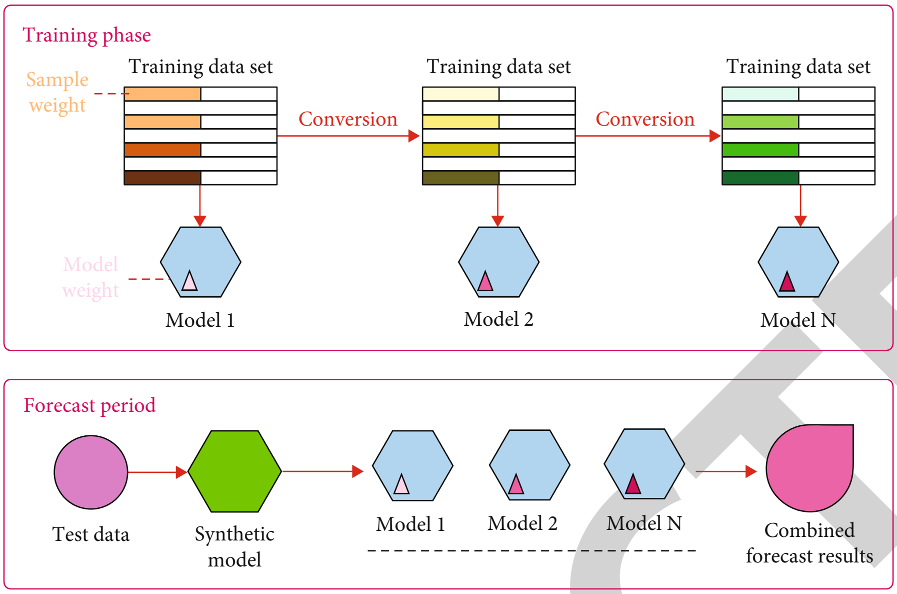

Figure 1: Common algorithms and redundancy elimination algorithms in encryption mathematical modeling teaching.

algorithm is designed according to the calculation results. Figure 1 shows the redundancy elimination algorithm commonly used in encryption mathematical modeling teaching.

2. Literature Review

The rapid development of technologies such as cloud computing, Internet of Things, and social networking has led to a rapid increase in network information flows from GB to TB, PB, EB, and even ZB [6]. The sheer size of the data, the rapid flow of data, the dynamic data system, the variety of data types, and the enormous value of big data have brought enormous impacts and challenges to the security and privacy of user information assets [7, 8]. Traditional data encryption storage and management methods have struggled to meet large data requirements in terms of encryption speed, storage capacity, and security [9, 10]. In addition, most data acquisition systems, such as satellite data signal acquisition, radar echo signal data acquisition, and digital video signal processing, require real-time and safe data transmission, which puts forward higher requirements for the transmission speed, storage speed, storage capacity, and security of the data acquisition and storage system [11, 12]. Secure storage of big data: the amount of data has increased from GB to EB and ZB and continues to grow explosively [13, 14]. According to IDC's report in March 2008, individual users just entered the TB era in 2006, and about 180 EB of data was generated worldwide: in 2007, the global new data volume was 281 EB, an increase of about 75% over the previous year, while the total capacity of all available storage media was 264 EB, and the new data volume has exceeded 6% of the capacity of all available storage media. The total amount of global data in 2011 was 10 times that in 2006, reaching 1.8 ZB [15]. In addition to the above typical examples, several other main sources of large-scale data are shown in Table 1:

In March 2009, a large number of Google users' data were stolen. In 2011, Nate, one of the three major portals in South Korea, and Saiwo, a social network, were attacked by hackers, resulting in the disclosure of 35 million user information: in April 2011, Sony's system vulnerability led to the theft of 77 million user data. On December 21, 2011, the data of 6 million users on CSDN, China's largest programmer community, was made public [16]. The files published by hackers contain a large number of user email accounts and password information. In August 2012, Shengda cloud enterprise lost a large amount of data of users due to virtual machine failure [17, 18]. Recently, Amazon has also constantly exposed various security incidents of big data in the cloud computing environment [19]. According to Gartner's 2012 survey report, more than 60% of enterprise CTOs believe that the main reason for not adopting cloud computing technology in the short term is that big data faces problems in security and privacy protection. From simple data to trade secrets to intellectual property rights, the disclosure of big data may lead to reputation damage, economic losses, and even legal sanctions [20].

In the process of big data security protection, potential threats may lead to some more basic threats. Common potential threats can be divided into the following four types: (1) eavesdropping, (2) traffic analysis, (3) information leakage caused by carelessness of operators, and (4) information leakage caused by media waste. Figure 2 shows some typical threats faced by big data and their relationship. The paths in the figure can be staggered. For example, counterfeiting attack can become the basis of all basic threats. At the same time, counterfeiting attack itself also has the potential threat of information disclosure.

The strength of big data security system is equal to that of its weakest link, and its security protection needs to combine different types of threat countermeasures. Therefore, the security protection technology of big data involves a very wide range of fields, including physical security, personnel security,

Table 1: Other sources of big data.

Serial number	Data category	Source
1	Sensor data	Sensor perception of environment
2	Click stream data	Click stream of users on the Internet
3	Mobile device data	Mobile phone, PDA, navigation, etc.
4	RFID data	Wide application of RFID

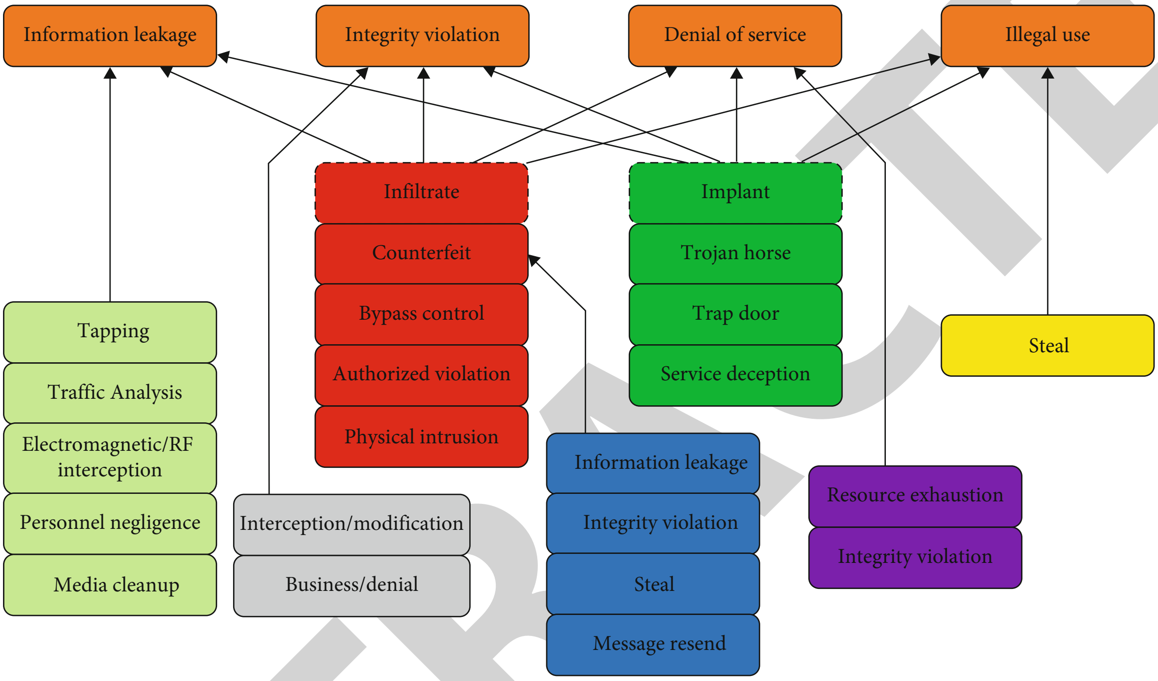

Figure 2: Typical threats and their relationships.

management security, media security, radiation security, and life cycle security (the process from the generation of big data to the demise of big data is called the life cycle of big data). No matter which link, big data encryption algorithm is the basis for the protection of big data. Limited to space, this paper only discusses the security problems related to big data encryption algorithms. Considering the existing powerful cryptographic analysis methods, such as differential cryptographic attack, linear cryptographic attack, integral attack, algebraic attack, man in the middle attack, and related key attack, we have to consider using more complex encryption algorithms and protective measures to protect the security of big data. To sum up, the amount of data in the era of big data increases nonlinearly. The increasing amount of data makes the traditional security and encryption tools no longer as effective as before. Modern cryptosystems are mostly designed for the needs of text data encryption and are not well combined with the characteristics of big data, so it is difficult to meet the actual application needs [21, 22]. The secure storage and data protection of big data are facing unprecedented pressure and challenges. Simply relying on increasing encryption, storage devices and bandwidth cannot fundamentally solve the problem, and new technical solutions must be sought. Based on this, this paper proposes a scheme that can meet the symmetric cryptographic algorithm and asymmetric encryption algorithm of big data and makes a new attempt for attribute encryption of big data.

3. Research Methods

3.1. Big Data Redundancy Elimination Algorithm Based on Similarity Calculation. In the space of data structure Bloom filter, it has the advantages of high data compression efficiency. The eigenvalue of the algorithm is composed of the representation of the Bloom filter data structure [23]. Compared with the traditional data redundancy elimination algorithm, the Bloom filter algorithm has more advantages in query time and space efficiency and is more suitable for processing large data.

Assuming that a certain data is a shingle, the construction method of the Bloom filter can be formed according to the following points:

(1) Construct BF data structure, where the structure is m bits and the initial value of all data is 0

(2) Suppose that the mapping function is two hash functions, including hASH1 and hASH2 functions

(3) Use the two functions in (2) to calculate the summary value in each shingle, and on this basis, set the bit value corresponding to BF as 1

(4) The characteristic value of the file is BF of the output

According to the above research and analysis, in the process of calculating the similarity of big data, this paper uses the Hamming distance to determine the similarity through the Bloom filter. The Hamming solution method mainly calculates the corresponding different numbers in two binary sequences. In addition, there are four methods to solve the similarity, namely, cosine, overlap, dice, and Jaccard. The calculation method is shown in

$$\text{Cosine\_sim}(x, y) = \frac{\bar{X} \cdot \bar{Y}}{\left\|\bar{X}\right\| \cdot \left\|\bar{Y}\right\|} = \frac{\sum_{i=1}^{n} X_i Y_i}{\sqrt{\sum_{i=1}^{n} X_i^2 \sum_{i=1}^{n} Y_i^2}}, \quad (1)$$

$$\text{Overlap\_sim}(x, y) = \frac{\sum_{i=1}^{n} X_i Y_i}{\min\left(\sum_{i=1}^{n} X_i^2, \sum_{i=1}^{n} Y_i^2\right)}, \quad (2)$$

$$\text{Dice\_sim}(x, y) = \frac{2\sum_{i=1}^{n} X_i Y_i}{\sum_{i=1}^{n} X_i^2 + \sum_{i=1}^{n} Y_i^2}, \quad (3)$$

$$\text{Jaccard\_sim}(x, y) = \frac{\sum_{i=1}^{n} X_i Y_i}{\sum_{i=1}^{n} X_i^2 + \sum_{i=1}^{n} Y_i^2 - \sum_{i=1}^{n} X_i Y_i}. \quad (4)$$

In formula, $\text{sim}(x, y)$ represents the similarity function. $\bar{X} \cdot \bar{Y} = \sum_{i=1}^{n} X_i Y_i$. According to the above process, the similarity between the two big data can be calculated.

Data redundancy elimination technology is also known as data compression technology [24–26]. The working principle of redundancy elimination technology is to delete two or more duplicate data in a data set to ensure that only the same data in the last data set is retained, so that the deleted redundant data will be replaced by data pointer. In this process, the data blocks in the data set will be shared by multiple data files at the same time, and the sharing relationship is shown in Figure 3.

According to Figure 3, in the data redundancy storage system, if a data block is damaged, multiple files may be unavailable at the same time. In the process of big data attribute encryption, the data storage space can be optimized through data redundancy elimination technology. Therefore, deleting the same data block in the data set in the processing process can reduce the workload of data encryption and improve the efficiency of data encryption. In addition, after deleting the redundant data in the data set, the data compression efficiency is improved and the number of transmitted data is reduced, so that the bandwidth of the transmission channel can be fundamentally alleviated.

When judging the reduction rate of data, it is mainly realized by the ratio of the number of bytes before the deletion of redundant data to the number of bytes processed. According to this result, the DER calculation formula is as follows:

$$\text{DER} = \frac{\text{Bytes In}}{\text{Bytes Out}}, \quad (5)$$

where data elimination ratio (DER) represents the discernible coding rule, bytes is the number of bytes, Bytes Out represents byte output, and Bytes In represents byte input. In general, the value of DER can be determined according to two conditional factors; that is, it does not strictly consider the overall cost of the original data. In order to better optimize the data overhead and optimize the calculation formula of data reduction rate, set DER as

$$\text{DER} = \frac{\text{DER}}{1 + f}. \quad (6)$$

In this way, according to the calculation results of the above formula, we can know that the cost of the original data is f, and its calculation method is shown in

$$f = \frac{\text{Metadate Size}}{\text{Average ChunkSize}}, \quad (7)$$

where Metadate Size represents the metadata size and Average ChunkSize represents the average block size.

3.2. Proposal of Big Data Encryption Algorithm. According to the above data similarity calculation results, this paper proposes an elliptic curve encryption algorithm (ECC) to realize the encryption of big data. The algorithm has the advantages of low computational overhead and high encryption security performance in the encryption process. The encryption principle security of the algorithm is based on the difficulty of curve discrete logarithm (ECDLP). Because ECC algorithm can use relatively short key to obtain the corresponding encryption security in practical application, it can fundamentally reduce part of the overhead in the overall calculation process.

The evaluation indexes of block cipher working mode mainly include the security performance of data encryption, the application performance after encryption, and the characteristic points in the calculation process, which are specifically expressed as follows:

(1) Safety performance

 (a) After encrypting the data, the data set can resist the attack

 (b) Whether the overall security of the data set can be verified

 (c) Whether the statistical characteristics of the output information of encrypted data are random

(2) Application performance after encryption: this performance index mainly refers to the effectiveness in the calculation process, whether the storage space requirements are met, and the data preprocessing ability

(3) Execution feature: this feature mainly refers to the password services that can be provided

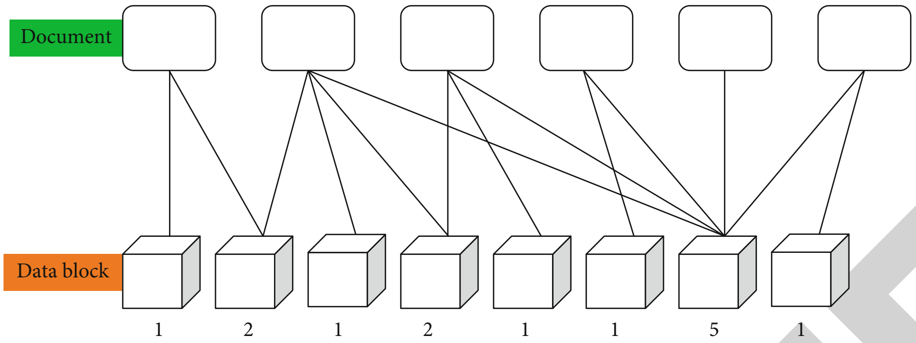

Figure 3: Relationship between file and data block.

The ECC offers an encryption scheme that combines the characteristics of an encryption algorithm and a block cipher algorithm to fully satisfy a combination of symmetric encryption algorithms and asymmetric encryption algorithms in a large data encryption process. The mathematical model of attribute encryption is presented in Figure 4.

3.3. Redundant Data Detection. Excess data detection is used to detect additional data that needs to be encrypted, and then the duplicate data in the data is deleted according to the detection results. The size of the data is described as the total number of files. The execution steps are as follows:

(1) Initialize the contents in the hash function table, and on this basis, use the data file complete detection algorithm. In the process of detection and calculation, this paper will take the data file that needs to be encrypted separately as the granularity, preliminarily detect the duplicate data in the data file, and then get the hash function value according to the detection results

(2) Compare the results of the values in the steps above with the results of the values stored in the hash function table. If the two values are the same or the error between them is within a reasonable, acceptable range, use the pointer to replace one of the files. If the matching values are different or the error is too large, it is two completely different data files, and the two data files need to be stored separately

(3) In the complete document detection method, the data files that do not repeat each other are rearchived. In the process, this paper will use the CDC data block calculation method to archive them one by one from the source of the file

(4) Input the data file after the archive partition into the data transmission stream in different areas again, and use the Bloom filter data structure to detect the data

3.4. Plaintext Encryption after Preprocessing. In the actual calculation process, the key length is 128192256 bits and the packet length is 128 bits. The calculation process is as follows:

(1) Numerical initialization

Here, the 128 bit message packet is divided into 16 bytes and marked as

$$\text{Inputblock} = m_0, m_1, \cdots, m_{15}. \tag{8}$$

According to the calculation result of the above formula, the key grouping formula is expressed as

$$\text{InputKey} = m_0, m_1, \cdots, m_{15}, \tag{9}$$

where Inputblock represents the input module, InputKey represents the input key, m represents the input byte, and the internal data structure is

$$\text{Inputblock} = \begin{pmatrix} m_0 & m_4 & m_8 & m_{12} \\ m_1 & m_5 & m_9 & m_{13} \\ m_2 & m_6 & m_{10} & m_{14} \\ m_3 & m_7 & m_{11} & m_{15} \end{pmatrix}, \tag{10}$$

$$\text{InputKey} = \begin{pmatrix} k_0 & k_4 & k_8 & k_{12} \\ k_1 & k_5 & k_9 & k_{13} \\ k_2 & k_6 & k_{10} & k_{14} \\ k_3 & k_7 & k_{11} & k_{15} \end{pmatrix}. \tag{11}$$

(2) Internal function (State) solution

In general, the internal function is described as any byte in State. Generally, x gives a nonlinear replacement byte, in which random non-0 byte $x \in F_{28}$ may be replaced by y:

$$y = \frac{A}{x} + b. \tag{12}$$

4. Result Analysis

4.1. Algorithm Performance Comparison. Simulations have been developed to further validate the practical effectiveness

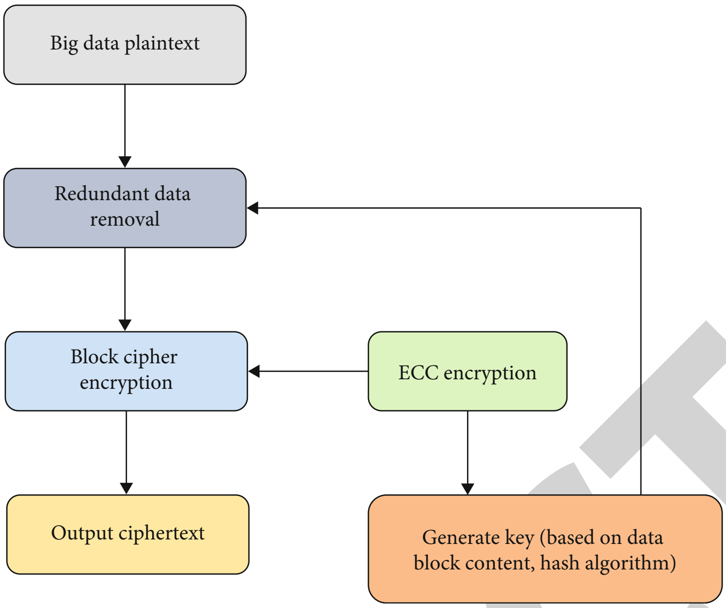

Figure 4: Model of large data encryption algorithm based on data resource technology.

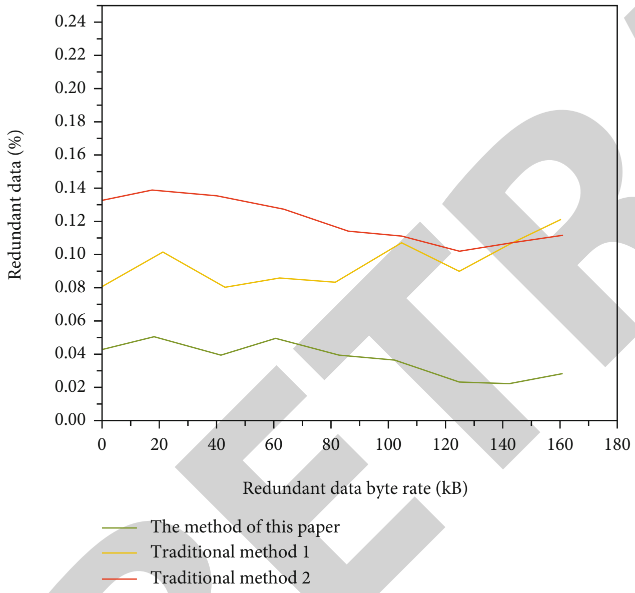

Figure 5: Comparison of different redundancy rate monitoring methods.

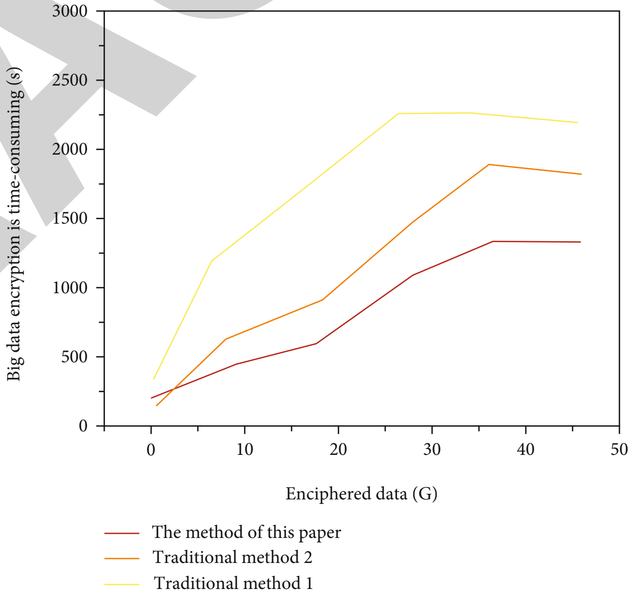

Figure 6: Comparison of encryption time of different methods.

of the proposed method. Traditional method 1 and traditional method 2 are the control group of this experiment, and the experimental results of different methods are compared. The comparison index is redundant data detection rate and encryption time. The comparison results are shown in Figure 5.

As shown in Figure 5, the probability of redundant data in the traditional method is high. During the whole experiment, the approximate fluctuation range is 0.08%-0.14%, which is not only high but also large. In contrast, under the condition of different redundant data byte rate, the occurrence probability of redundant data is less than 0.05%, which is far lower than the two traditional methods; this suggests that the proposed method has good application performance.

In the process of encrypting data attributes, the actual simulation environment uses a PC with AMD Athlon (TM) IIX3, 3.10 GHz and 2 GB storage space, in which the programming language is C +. On this basis, three methods are used to compare the encryption time for files with file sizes of 1G, 5G, 10G, 30G, and 50G. The shorter the encryption time, the higher the efficiency of this method. The experimental comparison results are shown in Figure 6.

According to Figure 6, compared with the two traditional literature methods in terms of data encryption time, the algorithm in this paper takes less time to encrypt data of different sizes than the traditional method, and the encryption time does not increase due to the excessive amount of encrypted data, while the literature method will increase the encryption time with the increase of encrypted data. In conclusion, the algorithm in this paper is more applicable.

5. Conclusion

At this stage, traditional large data character encryption methods do not meet the basic needs of the industry. Based on this, this paper proposes a new method of mathematical modeling of encryption of large data properties based on information resource technology. Based on the Bloom filter, a large data redundancy algorithm was developed, an elliptical encryption algorithm was proposed based on the data redundancy results, and a scheme and asymmetric encryption algorithm were developed that met the big data symmetric encryption algorithm. A mathematical model of encryption of large data properties was developed. The simulation results show that the method presented in this document has the advantage of low computation and encryption time and high efficiency in detecting redundant data. The results of the experiment show that the proposed method has good application value and is a reliable basis for in-depth study in this area.

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 they have no conflicts of interest.

References

[1] J. H. Lee and H. Y. Kwon, “Redundancy analysis and elimination on access patterns of the windows applications based on I/O log data,” *IEEE Access*, vol. 8, pp. 40640–40655, 2020.

[2] C.-L. Huang, Y. Jiang, and W.-C. Yeh, “Developing model of fuzzy constraints based on redundancy allocation problem by an improved swarm algorithm,” *IEEE Access*, vol. 8, pp. 155235–155247, 2020.

[3] L. Ye, Y. Yang, X. Jing, J. Ma, and H. Li, “Single-satellite integrated navigation algorithm based on broadband LEO constellation communication links,” *Remote Sensing*, vol. 13, no. 4, p. 703, 2021.

[4] D. Wang, W. Cui, and B. Qin, “Graph compression storage based on spatial cluster entity optimization,” *IEEE Access*, vol. 8, pp. 29075–29088, 2020.

[5] H. Bi, W.-L. Shang, Y. Chen, and K. Wang, “Joint optimization for pedestrian, information and energy flows in emergency response systems with energy harvesting and energy sharing,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 5, pp. 1–15, 2022.

[6] X. Zhou, X. Xu, W. Liang et al., “Intelligent small object detection for digital twin in smart manufacturing with industrial cyber-physical systems,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 2, pp. 1377–1386, 2022.

[7] M. Selvi and B. Ramakrishnan, “Lion optimization algorithm (LOA)-based reliable emergency message broadcasting system in VANET,” *Soft Computing*, vol. 24, no. 14, pp. 10415–10432, 2020.

[8] J. Li, R. Zhang, Y. Liu, Z. Zhang, and W. Liu, “The method of static semantic map construction based on instance segmentation and dynamic point elimination,” *Electronics*, vol. 10, no. 16, article 1883, 2021.

[9] Z. Cai and X. Zheng, “A private and efficient mechanism for data uploading in smart cyber-physical systems,” *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2020.

[10] X. Zheng and Z. Cai, “Privacy-preserved data sharing towards multiple parties in industrial IoTs,” *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 968–979, 2020.

[11] S. Abdulateef, N. A. Khan, B. Chen, and X. Shang, “Multidocument Arabic text summarization based on clustering and Word2Vec to reduce redundancy,” *Information*, vol. 11, no. 2, p. 59, 2020.

[12] B. Yang, X. Li, Y. Hou et al., “Non-invasive (non-contact) measurements of human thermal physiology signals and thermal comfort/discomfort poses-a review,” *Energy and Buildings*, vol. 224, article 110261, 2020.

[13] X. Cheng, B. Yang, A. Hedman, T. Olofsson, H. Li, and L. Van Gool, “NIDL: a pilot study of contactless measurement of skin temperature for intelligent building,” *Energy and Buildings*, vol. 198, pp. 340–352, 2019.

[14] S. Kundu, A. D. Burman, S. K. Giri, S. Mukherjee, and S. Banerjee, “Selective harmonics elimination for three-phase seven-level CHB inverter using backtracking search algorithm,” *International Journal of Power Electronics*, vol. 11, no. 1, pp. 1–19, 2020.

[15] O. Abdel Wahab, A. Mourad, H. Otrok, and T. Taleb, “Federated machine learning: survey, multi-level classification, desirable criteria and future directions in communication and networking systems,” *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1342–1397, 2021.

[16] H. Sami, A. Mourad, and W. El Haj, “Vehicular-OBUs-as-on-demand-fogs: resource and context aware deployment of containerized micro-services,” *IEEE/ACM Transactions on Networking*, vol. 28, no. 2, pp. 778–790, 2020.

[17] E. Y. Baagyere, A. N. Agbedemnab, Q. Zhen, M. I. Daabo, and Z. Qin, “A multi-layered data encryption and decryption scheme based on genetic algorithm and residual numbers,” *IEEE Access*, vol. 8, pp. 100438–100447, 2020.

[18] M. H. Saracevic, S. Z. Adamovic, V. A. Miskovic, M. Elhoseny, and K. Shankar, “Data encryption for internet of things applications based on catalan objects and two combinatorial structures,” *IEEE Transactions on Reliability*, vol. 70, no. 2, pp. 819–830, 2021.

[19] L. Teng, H. Li, S. Yin, and Y. Sun, “A modified advanced encryption standard for data security,” *International Journal of Network Security*, vol. 22, no. 1, pp. 112–117, 2020.

[20] P. Kumar and A. K. Bhatt, “Enhancing multi-tenancy security in the cloud computing using hybrid ECC-based data encryption approach,” *IET Communications*, vol. 14, no. 18, pp. 3212–3222, 2020.

[21] N. Nguyen, L. Pham, M. B. Nguyen, and G. Kaddoum, “A low power circuit design for chaos-key based data encryption,” *IEEE Access*, vol. 8, pp. 104432–104444, 2020.

[22] X. Yan, C. Yang, Q. Zhang, and J. Yu, “Revocable ciphertext-policy attribute-based encryption in data outsourcing systems

from lattices," *International Journal of Embedded Systems*, vol. 13, no. 4, p. 414, 2020.

[23] R. Huang, P. Yan, and X. Yang, "Knowledge map visualization of technology hotspots and development trends in China's textile manufacturing industry," *IET Collaborative Intelligent Manufacturing*, vol. 3, no. 3, pp. 243–251, 2021.

[24] P. Ajay, B. Nagaraj, and J. Jaya, "Bi-level energy optimization model in smart integrated engineering systems using WSN," *Energy Reports*, vol. 8, pp. 2490–2495, 2022.

[25] Z. Lv and L. Qiao, "Deep belief network and linear perceptron based cognitive computing for collaborative robots," *Applied Soft Computing*, vol. 92, article 106300, 2020.

[26] Z. Lv, Y. Han, A. K. Singh, G. Manogaran, and H. Lv, "Trustworthiness in industrial IoT systems based on artificial intelligence," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 1496–1504, 2021.