Computers, Materials & Continua
DOI:10.32604/cmc.2022.019318
Article

Tech Science Press

Dynamic Encryption and Secure Transmission of Terminal Data Files

Ruchun Jia[1,*], Yang Xin[2], Bo Liu[3] and Qin Qin[4]

[1]Wangjiang Campus of Sichuan University, 610065, Chengdu, China
[2]Beijing University of Post and Telecommunications, 100876, Beijing, China
[3]National University of Defense Technology, 410073, Changsha, China
[4]Loughborough University, E20 3BS, London, Britain
*Corresponding Author: Ruchun Jia. Email: ruchunjia@zaibei.org.cn
Received: 09 April 2021; Accepted: 23 August 2021

Abstract: Data is the last defense line of security, in order to prevent data loss, no matter where the data is stored, copied or transmitted, it is necessary to accurately detect the data type, and further clarify the form and encryption structure of the data transmission process to ensure the accuracy of the data, so as to prevent data leakage, take the data characteristics as the core, use transparent encryption and decryption technology as the leading, and According to the data element characteristics such as identity authentication, authority management, outgoing management, file audit and external device management, the terminal data is marked with attributes to form a data leakage prevention module with data function, so as to control the data in the whole life cycle from creation, storage, transmission, use to destruction, no matter whether the data is stored in the server, PC or mobile device, provide unified policy management, form ecological data chain with vital characteristics, and provide comprehensive protection system for file dynamic encryption transmission, such as prevention in advance, control in the event, and audit after the event, so as to ensure the security of dynamic encryption in the process of file transmission, ensure the core data of the file, and help the enterprise keep away from the risk of data leakage.

Keywords: Terminal data; data anti disclosure; dynamic symmetric key; dncryption algorithm; secure transmission

1 Introduction

With the development of the era of big data, when we controlled data before, most of them are strongly controlled and they all are directly isolated or fully encrypted. We call it cage and shackle control, which brings a lot of unnecessary troubles in the actual data production, use, and flow [1]. People need to deal with data in a more flexible way. At this time, intelligent data security control came into being. The administrator can control the data according to the importance of the data [2]. Few people will pay attention to the content of the document, and the management of the data is relatively simple. Generally, it is full encryption and full authorization. The importance of the document is not

distinguished. However, with the development of the society, the format of the document is more and more, and owing to the continuous outbreak of security events, the degree of the attention people pay to the data has changed [3], and the data is divided into structured data and unstructured data. More attention is paid to the sensitive information in the document content, what are the applications of using documents, and different management and storage for different types of documents and documents with different contents. By using regular expression and hash table to find keywords, data leakage can be detected. With the development of network information transmission technology, a large number of files and data need to be transmitted on the network, and the security of file data transmission has attracted people's great attention. In the process of data terminal file transmission, it is easy to be invaded by plaintext, which leads the leakage of data terminal files. So it is necessary to design the secure transmission of data terminal file. Therefore, it is of great significance to study the encrypted and secure transmission of data terminal files to ensure the output security of data terminal files [4].

Combined with random coding design method, the design of secure transmission of data terminal files is based on the encryption design of data terminal files. Traditional data encryption methods mainly include ellipse encryption. By constructing the security key of the data terminal file information encryption, the ellipse encryption method adopts the arithmetic coding design scheme to design the self-adaptive feature classification and vector quantization coding of the data terminal file storage information [5]. Because the combination structure of the data terminal file is simple and the network space has the characteristics of self-organization, the security encryption performance of the data terminal file is not good, so it needs to be optimized to design the encryption key of data terminal file. Curve encryption method: firstly, build the secure transmission protocol model of data terminal file [6], Then, use encryption method to design the encryption of data terminal file, construct the key protocol of data terminal file encryption, Finally, combine arithmetic coding and encryption key construction method to realize the secure transmission of data terminal file, which can effectively reduce the data terminal file leakage of components, but redundant data will be generated [7].

For the above problems, in this paper, a research method based on dynamic encryption secure transmission of the terminal data anti disclosure file is proposed. It constructs security transmission ciphertext protocol of the data terminal file, uses the agent-free key release protocol to access the data terminal file control, increases the security of the file transmission process by designing dynamic symmetric key [8]. In the file level of data terminal, the data element feature filtering coding technology is implemented. Through real-time interception of reading or writing requests of file system, the file is dynamically tracked and transparently encrypted or decrypted. The encryption or decryption of the file is dynamic and transparent, which does not change the user's operating habits. The format and state of the original file are not changed due to the characteristics of the data itself, which is combined with the bilinear mapping method to design the key construction and arithmetic coding in the process of the security encryption of data terminal file. According to the strength of plaintext attack, the scrambling degree of dynamic symmetric key encryption of data terminal file is rearranged, which effectively solves the problem of data leakage in traditional methods and reduces the generation of redundant data. The simulation results show the advantages of this method in improving the secure encrypted transmission of data terminal files.

2 Encryption Structure of Data Terminal Against the Transmission of Leaked Files

2.1 Data Terminal Anti Disclosure File Protocol

In order to realize the secure transmission of data terminal files, the ciphertext protocol for the secure transmission of data terminal files is constructed firstly, and the access control of data terminal files is carried out by using the agent-free key release protocol [9]. The number of secure ciphertext transfer functions for the encryption of data terminal files in the limited domain is $Decrypt(sk, c^*)A = T = (t_{i,j})_{i,j=1}^{m}$, Where A is the encryption matrix and T is the control matrix. Based on the symmetric encryption algorithm to construct the key, the searchable encryption key of the data terminal file security transmission is obtained as follows:

$$Decrypt(sk, c^*)\boldsymbol{T}^{-1}\boldsymbol{A} = \begin{pmatrix} t_{1,1} & \cdots & t_{1,m} \\ \vdots & \ddots & \vdots \\ t_{m,1} & \cdots & t_{m,m} \end{pmatrix} \begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,m} \end{pmatrix} \tag{1}$$

A method supporting access control is used to authorize encryption control of unencrypted data in data terminal files, and a structural analysis model of data terminal files is constructed to obtain the proxy re-encryption key protocol of data terminal files:

$$\begin{aligned} &Decrypt(sk, c^*)(\boldsymbol{T}^{-1})^{(\alpha_1^{-1},\cdots,\alpha_m^{-1})^T}\boldsymbol{A}^{(\alpha_1,\cdots,\alpha_m)} \\ &= \begin{pmatrix} {\alpha_1}^{-1}t_{1,1} & \cdots & {\alpha_1}^{-1}t_{1,m} \\ \vdots & \ddots & \vdots \\ {\alpha_m}^{-1}t_{m,1} & \cdots & {\alpha_m}^{-1}t_{m,m} \end{pmatrix} \begin{pmatrix} \alpha_1 a_{1,1} & \cdots & \alpha_m a_{1,m} \\ \vdots & \ddots & \vdots \\ \alpha_1 a_{m,1} & \cdots & \alpha_m a_{m,m} \end{pmatrix} \end{aligned} \tag{2}$$

Considering the randomness of the parameters, the encryption key is reset, and the length of the key is n. The re-encryption key protocol is used to expand the key, and the key expansion sequence is obtained $X = x_1, x_2, \ldots, x_n$, In the process of keyword ciphertext search, the proxy re encrypted ciphertext of data terminal file is obtained as $S_n = x_1 + x_2 + \ldots + x_n$, Use its own private key for ciphertext reorganization, output as:

$$Decrypt(sk, c^*)\boldsymbol{A}\boldsymbol{A}^{-1} = \begin{pmatrix} t_{1,1} & \cdots & t_{1,m} \\ \vdots & \ddots & \vdots \\ t_{m,1} & \cdots & t_{m,m} \end{pmatrix} \tag{3}$$

The key encryption algorithm is used for random linear processing of data terminal files [10], and the public key encryption sequence of data terminal files is as follows:

$$\begin{aligned} &Decrypt(sk, c^*)\boldsymbol{A}^{(\alpha_1,\cdots,\alpha_m)}Decrypt(sk, c^*)(\boldsymbol{A}^{-1}) \\ &= \begin{pmatrix} \alpha_1 a_{1,1} & \cdots & \alpha_m a_{1,m} \\ \vdots & \ddots & \vdots \\ \alpha_1 a_{m,1} & \cdots & \alpha_m a_{m,m} \end{pmatrix} \begin{pmatrix} {\alpha_1}^{-1}t_{1,1} & \cdots & {\alpha_1}^{-1}t_{1,m} \\ \vdots & \ddots & \vdots \\ {\alpha_m}^{-1}t_{m,1} & \cdots & {\alpha_m}^{-1}t_{m,m} \end{pmatrix} \end{aligned} \tag{4}$$

Linear encryption is applied to the specified keywords to get the characteristic distribution value of ciphertext protocol $e = h(m)$, The key ciphertext is used to return to the user, and the arithmetic

coding is designed [11–13], and the quantitative characteristic equation of data terminal file security transmission is obtained:

$$Decrypt(sk, c^*)(\boldsymbol{A}^{(\alpha_1,\cdots,\alpha_m)})^{-1} = e \cdot \begin{pmatrix} {\alpha_1}^{-1} t_{1,1} & \cdots & {\alpha_1}^{-1} t_{1,m} \\ \vdots & \ddots & \vdots \\ {\alpha_m}^{-1} t_{m,1} & \cdots & {\alpha_m}^{-1} t_{m,m} \end{pmatrix} = e \cdot (\boldsymbol{A}^{-1})^T \tag{5}$$

Based on this, a ciphertext protocol for secure file transmission of data terminal is constructed. Combined with the elliptic linear construction method [14–16], the ciphertext transmission structure model of data terminal file encryption is obtained as shown in Fig. 1.

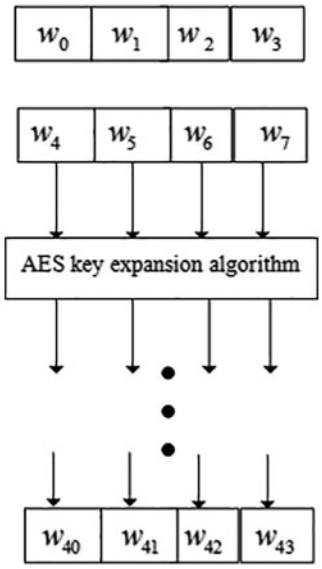

Figure 1: Ciphertext transmission structure model of data terminal file encryption

2.2 Dynamic Key Construction

This paper constructs the dynamic symmetric key of the data terminal file, combines the bilinear mapping method to construct the key and design the arithmetic coding in the process of data terminal file security encryption. According to the indistinguishability of the ciphertext, the hash function of data terminal file encryption is obtained as follows $P(x)$:

$$\begin{aligned} P(x) &= 2[1-\varphi(S_{obs})] \\ &= 2\left(1-\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{S_{obs}} e^{-2}dx\right) \\ &= \frac{2}{\sqrt{2\pi}}\int_{S_{obs}}^{+\infty} e^{-2}dx \\ &= \frac{2}{\sqrt{\pi}}\int_{\frac{S_{obs}}{\sqrt{2}}}^{+\infty} e^{-2}dx \\ &= \left(\frac{S_{obs}}{\sqrt{2}}\right) \end{aligned} \tag{6}$$

If statistics $S_{obs} \geq 0.01$, Open system public parameters meet

$\varphi \in \{0, 1\}$, Represented as a 1-bit encoding map, the data owner will first select a random value to obtain the linear encoding feature distribution function of the data terminal file:

$$f(I) = \begin{cases} p(x) * I, & s = 0 \\ 1 - (1 - p(x)) * I, & s = 1 \end{cases} \tag{7}$$

Inside, I indicates the private key of the file sender of the data terminal, and sets the initial value $I = [0, 1]$, With any sender dividing the plaintext message into n blocks, using the dynamic symmetric key encryption method, the public key encryption protocol is obtained as follows:

$$f(x) = \begin{cases} x/P(x_1), & x \in I_1 \\ (x - P(x_1))/P(x_2), & x \in I_2 \\ \ldots \quad \ldots & \\ (x - \sum_{i=1}^{n-1} P(x_i))/P(x_n), & x \in I_n \end{cases} \tag{8}$$

Inside $P(x_i)(i = 1, \ldots, n)$ represents the probability interval of ciphertext distribution of data terminal file, constructs the arithmetic coding model of data terminal file according to the number of public key components, and obtains the key satisfaction:

$$f(x) = \frac{KC_1 \times KS_1}{f(I)} \tag{9}$$

Inside, KC_1 is the minimum value of the public key component, KS_1 Maximum value. Key design of dynamic symmetric key encryption with homomorphic encryption scheme, Take the inverse function of $f(x)$ as:

$$f^{-1}(x) = \begin{cases} P(x_1) \\ P(x_2) + P(x_1) \\ \ldots \\ P(x_n) + \sum_{i=1}^{n-1} P(x_i) \end{cases} \tag{10}$$

Read the ciphertext sequence to realize the dynamic symmetric key construction of the data terminal file, as shown in Fig. 2.

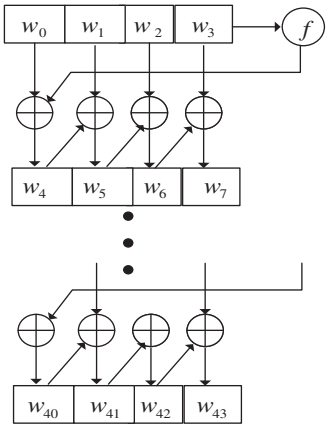

Figure 2: Dynamic symmetric key construction of data terminal file

3 Optimization of Encryption and Decryption Algorithm and Implementation of Secure Transmission

3.1 Encryption and Decryption Algorithm

On the basis of the above construction of ciphertext protocol for secure transmission of data terminal files, the design of dynamic symmetric key and the optimization of encryption algorithm are carried out . In this paper, the research method of secure transmission of dynamic encryption of data terminal files based on anti-leakage of data terminal is proposed, and the average mutual information function of encryption is designed by combining the bilinear mapping method for the key construction and arithmetic coding in the process of secure-encryption of data terminal files Number is:

$$H = -\sum_{i=1}^{n} \log_2(P(x_i)) \tag{11}$$

Coding extended sequences of bilinear maps $s = \{s_i, i = 1 \ldots M | s_i \in S\}$, The information entropy of homomorphic encryption is calculated as:

$$P_n = \frac{1}{M} card\{s_i | s_i = S_n\} \tag{12}$$

Inside, $S_n \in S, n = 1 \ldots N$, M is the number of traversal of the extended sequence, and the random permutation method is used to obtain the file security extended key of the data terminal $x = (x_1, \cdots, x_m)^T \in GF(2^n)^m$, Through key mapping, the encryption function of data terminal file security transmission is obtained as follows:

$$I^i = f^{-1}(x)(I^{i+1}) \tag{13}$$

$$size(I^i) = P(x_i) size(I^{i+1}) \tag{14}$$

The coding protocol for constructing data terminal file encryption in limited domain is **RkeyGen**$(param, rsk_{ID_i}, ID_i, ID_j)$, In the data terminal file combination sequence $x_1x_2x_3\ldots x_r$, According to the dynamic symmetric encryption key protocol, the public key of the nth encryption bit sequence is obtained $k_i, l_i \in Z_q^*$. Set the key of data terminal file encryption rk_{ij}, Make homomorphic public key $t_0 = H_1(g, g_1, g_2, g_3, h)$, Get the arithmetic coding protocol of data terminal file encryption:

$$\begin{aligned}&(rk_{1ij}, rk_{2ij}, rk_{3ij}, rk_{4ij}, rk_{5ij}, rk_{6ij})\\&= (g^{x_ik_i}, (g^{t_0}h)^{x_ik_i}, \tfrac{x_j}{x_i}, sr_i^{x_i^{-1}(t_0-t_i)}sr_j^{x_i^{-1}(t_j-t_0)}, k, g^{k_i})\end{aligned} \tag{15}$$

Inside:

$$k = e\left(g^{k_i}, g_1^{u_i(t_0-t_i)}g_1^{u_j(t_j-t_0)}\right)\frac{e(g^{k_i}, sk_{i1}g_1^{l_i})}{e((g^{t_0}h)^{k_i}, g^{u_i})}e(g, g_1)^{-k_il_i} \tag{16}$$

Using the closed-loop encryption method of integer polynomial, the output encryption result is:

$\mathrm{C} \rightarrow \mathrm{S}$: ClientHello{$\mathrm{Ver_c}$, $\mathrm{CipherSuite_c}$, R_c, SessionID}

$\mathrm{S} \rightarrow \mathrm{C}$: ServerHello{$\mathrm{Ver_s}$, $\mathrm{CipherSuite_s}$, R_s, SessionID}

The decryption algorithm is:

Decrypt (sk,c^*,z): The ciphertext of the data terminal file is q_0, When satisfied $q_0 \leftarrow \mathbb{Z} \cap [0,2^\gamma/\pi)$, Dynamic symmetric key for secure file transfer of data terminal $\overrightarrow{m} = (m_{ij})$, the output decryption key is: $param = \{G_1, G_2, e, g, g_2, g_3, h, H_1, H_2\}$, Therefore, the encryption and decryption algorithm design of data terminal file security transmission is realized.

3.2 Data Terminal File Security Transmission

The linear bit stream model of data terminal file security encryption is given as follows $s = \{s_i, i = 1\ldots M | s_i \in S\}$, Initialize the sensitive characteristic coefficient, and the dynamic symmetric key of file encryption is:

$\mathrm{C} \rightarrow \mathrm{S}$: Certificate{$\mathrm{Cert_c}$}

$\mathrm{C} \rightarrow \mathrm{S}$: ClientKeyExchange{K_c}

$\mathrm{C} \rightarrow \mathrm{S}$: CertificateVerify{{hash(messages)}$_{P_c^{-1}}$}

Combined with homomorphic encryption scheme, the optimal transmission control equation of the file is obtained as follows:

$$B(x) = \begin{cases} x \cdot p_n, & x \in [0, p) \\ (1-x) \cdot p_n, & x \in [p, 1] \end{cases} \tag{17}$$

In the process of data terminal file security transmission and encryption, the key construction and self-adaptive coding are realized by p parameters. According to the strength of plaintext attack, the scrambling degree of dynamic symmetric key encryption of data terminal file is rearranged. The

random linear coding method is used to realize dynamic symmetric key encryption of data terminal file.

4 Simulation Experiment and Result Analysis

In order to test the performance of this method in the implementation of data terminal file security encryption, a simulation experiment is carried out. Through regular expression detection (identifier), keyword and keyword pair detection, document attribute detection, the basic detection method uses the conventional detection technology to search and match the content, and the more common ones are regular expression and keyword. These two methods can make clear sensitive information content be detected; document attribute detection is mainly aimed at document type, document size and document name. The detection of document type is based on file format rather than suffix name. For the scenario of modifying suffix name, file type detection can accurately detect the type of detected file, And we can identify the document of special file type format through custom features. The experiment is designed with MATLAB 7, The length of random coding sequence of file data of data terminal is 1024, The length of the plaintext bit sequence is 200, The strength of plaintext attack is 20 dB, The initial sequence of encrypted bits is:

10101001010010101001100101000010011110100101111011101000010001111001111001011110 0

11111111101001111110011101110000001101011011 0

Set the encryption parameters of the data terminal file as the initialization parameters, and conduct the data terminal file encryption simulation according to the parameter settings in Tab. 1.

Table 1: Experimental parameter settings

Parameter setting	t_0	M	l	e	φ
Parameter value	54	43	15	0.56	0.52

Inside, t_0 is homomorphic public key, M is the number of iterations of the extended sequence, l is the public key of the encryption, e is the characteristic distribution value, φ 22 is public system parameter.

Build the dynamic symmetric key of the data terminal file, use the random linear encoding method to realize the dynamic symmetric key encryption of the data terminal file, and get the test results of the encryption performance of the terminal file as shown in Fig. 3.

Analysis of Fig. 3 shows that unencrypted files can be easily detected, with poor transmission security. However, for encrypted files, the longer the bit sequence is divided into blocks, the lower the transmission recognition rate is, Focus on the mandatory encryption, the transparency of use, the thoroughness of confidentiality, the application independence, and the flexibility of expansion. Use the terminal data element feature filtering and coding technology. Therefore, the method in this paper has better performance in encrypting and secure transmission of data terminal files, stronger anti attack ability, and improved the secure transmission performance of files.

In order to further verify the encryption effect of this method, we use literature [10] method, literature [12] method and this method to detect the encryption time-consuming, and the result is shown in Fig. 4.

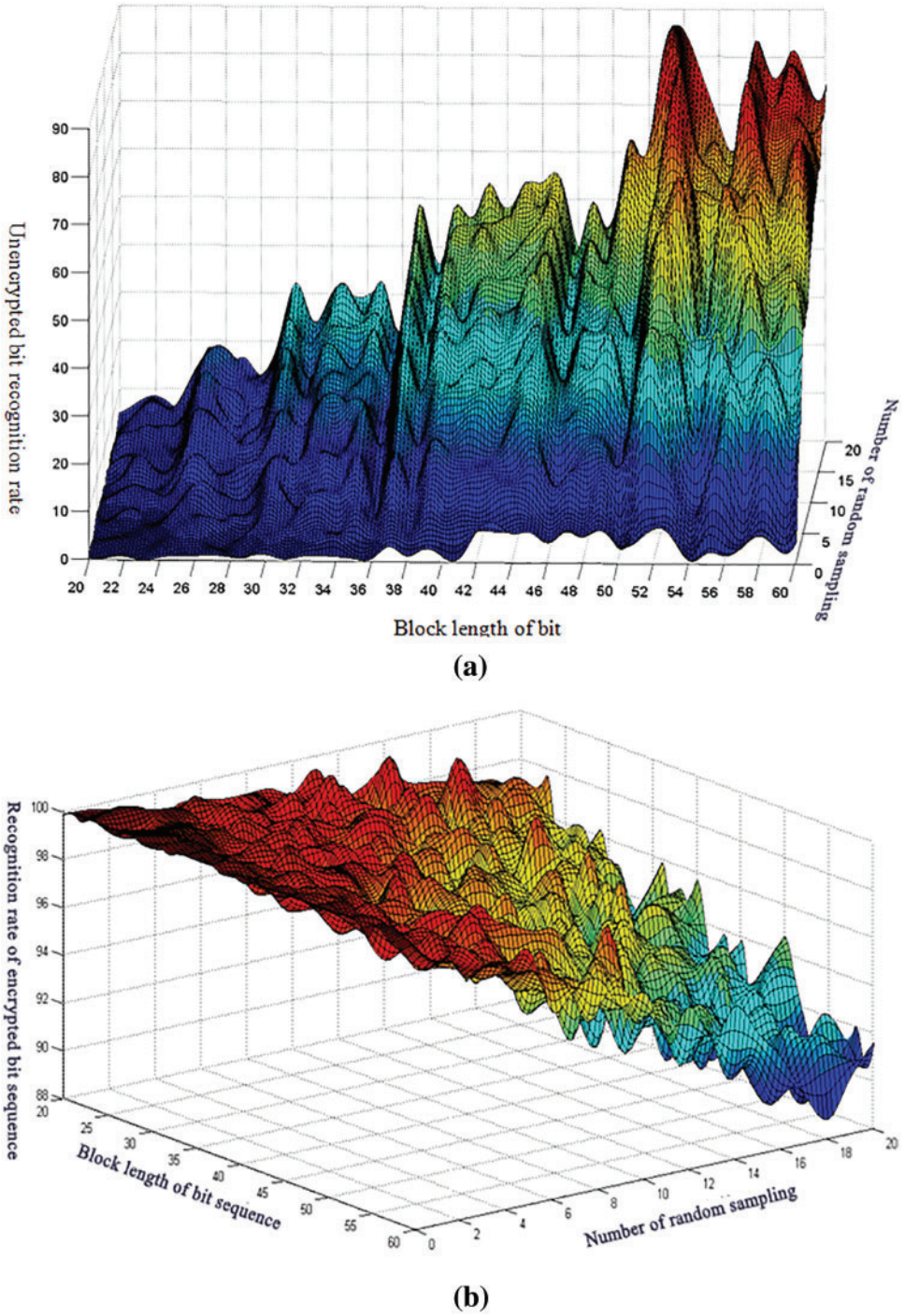

Figure 3: Encryption performance test. (a) Test results without file, (b) Encrypted file detection results

Analysis of Fig. 4 shows that the larger the file is, the longer the file encryption time is. When the file size is 15 KB, the encryption time of document [10] method is 13 s, that of document [12] method is 17 s, and that of this method is 1 s. When the file size is 50 KB, the encryption time of document

method is 27 s, the encryption time of document method is 36 s, and the encryption time of this method is 2S. The encryption time of this method is always shorter and the encryption efficiency is higher.

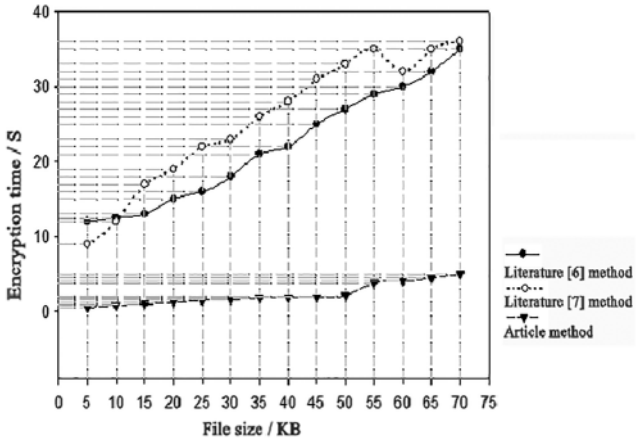

Figure 4: Comparison of encryption time in different methods

The data integrity of file transfer under different methods is tested, and the test results are as follows.

According to Fig. 5, file size is related to data transmission integrity. When the file size is 15 KB, the data transmission integrity of document [10] method is 75%, the data transmission integrity of document [12] method is 69%, the data transmission integrity of this method is 94%, and the data integrity of this method is high. When the file size is 60 KB, the data transmission integrity of document [10] method is 78%, the data transmission integrity of document [12] method is 68%, and the data transmission integrity of our method is 93%. The data integrity of this method has been kept at a high level, which shows that this method can resist external attacks in the transmission process.

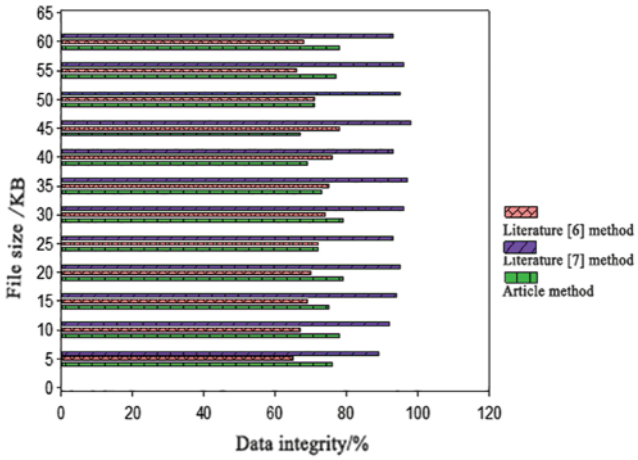

Figure 5: Data integrity transmitted by different methods

5 Epilogue

This paper takes data as the core, realizes the unified definition of data in data registration center, data authority center and data exception center through data element feature collection, It manages and serves various applications through data application unit and establishes a large platform of data and an ecosystem of fragmented application to explore beneficially the whole structure of software. Thus, digital right management is realized in the secure transmission of dynamic encryption based on terminal data anti disclosure file, DRM), which can realize automatic protection in the transient of sensitive data file generation, storage and transmission, as well as prevent the illegal replication, leakage and diffusion of sensitive data through conditional access control strategy, and realize the close combination of data authority control and business through fine-grained operation control and identity control strategy, which has an impact on the existing business process of users. The encryption method is used to design the encryption of data terminal file, construct the key protocol of data terminal file encryption, combine the arithmetic coding and encryption key construction method to realize the safe transmission of data terminal file, and draw the following conclusions through the experimental results:

(1) In the process of data transmission, the encrypted file can be effectively encrypted, the bit sequence becomes longer, the transmission recognition rate is reduced, and it has high security.
(2) When the file size is 50 KB, the encryption time of this method is only 2S. This method has a shorter encryption time and a higher encryption efficiency.
(3) When the file size is 60 KB, the data transmission integrity of this method is 93%. The data integrity of this method has been kept at a high level, and has a strong ability to resist external attacks.

To sum up, this method has better anti attack performance in data terminal file encryption and higher file transmission security.

Because of the randomness, energy limitation and time delay sensitivity of file transfer, how to solve these problems will be further studied in the future.

Funding Statement: The work was funded by Scientific Research Project of Sichuan Provincial Department of Education (13zao125), Comprehensive Reform Project of Software Engineering (zg−1202), Enterprise Informatization and Internet of Things Measurement and Control Technology Open Fund Project of Sichuan University Key Laboratory (2014wzy05).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] C. Li, Y. Xu, J. Tang and W. Liu, "Quantum blockchain: A decentralized, encrypted and eistributed eatabase based onquantum mechanics," *Journal of Quantum Computing*, vol. 1, no. 2, pp. 49, 2019.
[2] C. Wang and Y. Yuan, "An efficient ciphertext-policy attribute-based encryption scheme with policy update," *Computers, Materials & Continua*, vol. 63, no. 2, pp. 1031–1041, 2020.
[3] Y. Liu, Y. Ren, Q. Wang and J. Xia, "The development of proxy re-encryption," *Journal of Cyber Security*, vol. 2, no. 1, pp. 1–8, 2020.
[4] Y. Shah, D. Sehgal and J. K. Valadi, "Recent trends in antimicrobial peptide prediction using machine learning techniques," *Bioinformation*, vol. 13, no. 12, pp. 415, 2017.

[5] S. Hao, Y. Lü, J. Liu, Y. Liu and D. Xu, "Application of classified protection of information security in the information system of air pollution and health impact monitoring," *Journal of Hygiene Research*, vol. 47, no. 1, pp. 103–107, 2018.
[6] G. Cherubin, "Bayes, not naïve: Security bounds on website fingerprinting defenses," *Proceedings on Privacy Enhancing Technologies*, vol. 2017, no. 4, pp. 215–231, 2017.
[7] W. Fang, L. Pang and W. N. Yi, "Survey on the application of deep reinforcement learning in image processing," *Journal on Artificial Intelligence*, vol. 2, pp. 39–58, 2020.
[8] W. Fang, F. Zhang, Y. Ding and J. Sheng, "A new sequential image prediction method based on LSTM and DCGAN," *Computers Materials & Continua*, vol. 64, no. 1, pp. 217–231, 2020.
[9] T. Shirakawa, N. Sugiyama, H. Sato, K. Sakurai and E. Sato, "Gait analysis and machine learning classification on healthy subjects in normal walking," *International Journal of Parallel, Emergent and Distributed Systems*, vol. 32, no. 2, pp. 185–194, 2017.
[10] Y. Chen, Y. Zhou, X. Wang and L. Guo, "Video information hiding algorithm based on diamond coding," *Computer Application Research*, vol. 37, no. 10, pp. 2806–2812, 2017.
[11] Z. Chen, X. Huang and Z. Chen, "Interval multi-objective optimization algorithm for non dominated sorting cloud model," *Computer Engineering and Application*, vol. 53, no. 22, pp. 143–149, 2017.
[12] J. Li, K. Yue and J. Cai, "Ranking method of diversity graph based on distance measurement," *Journal of Software*, vol. 29, no. 3, pp. 599–613, 2018.
[13] L. Yang, Z. Kong and H. Shi, "Software definition: Dynamic deployment strategy of spatial information network multi controller," *Computer Engineering*, vol. 44, no. 10, pp. 58–63, 2018.
[14] N. S. Safa, C. Maple, T. Watson and S. Furnell, "Information security collaboration formation in organisations," *IET Information Security*, vol. 12, no. 3, pp. 238–245, 2017.
[15] Y. Li and Y. Li, "Intrusion detection algorithm of industrial control network based on self encoder and limit learning machine," *Journal of Nanjing University of Science and Technology*, vol. 43, no. 04, pp. 408–413, 2019.
[16] H. Chen, Y. Feng and X. Zhao, "Network intrusion detection method using SSO adaptive blacklist packet filter," *Control Engineering*, vol. 25, no. 10, pp. 1940–1945, 2018.