Research on Hybrid Encryption of Cross Border E-commerce Transaction Information Based on B+ Search Tree Algorithm

Jia-hua Li(✉)

School of Information Engineering, Guangzhou Vocational and Technical University of Science and Technology, Guangzhou 510550, China
lijiahua21223@163.com

Abstract. In order to solve the problem of low security existing in the traditional information hybrid encryption method, a cross border e-commerce transaction information hybrid encryption method based on B+ search tree algorithm is proposed. In the cross border e-commerce trading platform, B+ search tree algorithm is used to retrieve the e-commerce trading data, process and cluster the e-commerce trading information. On this basis, idea and ECC are taken as the hybrid encryption algorithm types, and the hybrid encryption of cross border e-commerce trading information is realized through the steps of generating key and private key, key management and distribution, and key exchange in hybrid encryption. Compared with the traditional encryption method, the experimental results show that the decryption time of the hybrid encryption method designed in this paper is longer, and the amount of data error is reduced by 2.44 MB, which means that the security of the method is higher.

Keywords: B+ search tree algorithm · Cross border transactions · E-commerce transaction information · Hybrid encryption

1 Introduction

E-commerce is a new type of business activity which is emerging in the current economic and social state. E-commerce has two types of explanation, narrow sense and broad sense. In a narrow sense, e-commerce refers to the activities of commodity transaction between consumers and consumers, between consumers and enterprises, enterprises and enterprises through the Internet. In a broad sense, e-commerce refers to all the comprehensive e-commerce activities carried out through the Internet/Intranet/enterprise external network [1]. In recent years, with the further acceleration of globalization, e-commerce, as a product of market economy and financial industry development and integration, has been developed rapidly. According to the current transaction scale, the future global trade economy will be traded through the network in the next ten years [2]. Under the trend of global economic integration, e-commerce will be able to trade in the future, In the future, e-commerce will occupy a greater and larger part in economic and trade. With the development of computer network technology and information technology, human beings have entered the information society and

S. Wang et al. (Eds.): IoTCare 2021, LNICST 414, pp. 290–307, 2022.
https://doi.org/10.1007/978-3-030-94185-7_20

network economy era rapidly. The development of e-commerce is becoming more and more rapid [3]. According to the annual monitoring report of China's e-commerce industry in 2019–2020, the e-commerce market in China will maintain a high-speed development in 2020, with the transaction scale exceeding 18.1 trillion yuan, In 2020, the transaction volume of China online shopping market amounted to 3304.53 billion yuan, accounting for 13.2% of the total retail sales of social consumer goods, with the penetration scale of online shopping users reaching 56.9%. Online transaction has become a mainstream consumer category. The trading platform emerges like a springing up. Nowadays, the mainstream trading platforms include tmall, Taobao, JD, etc., and the trading scale is expanding [4]. Therefore, a large amount of data is generated, and the security of cross border e-commerce transaction information is also seriously threatened. Therefore, the encryption method of cross border e-commerce transaction information is proposed by using cryptography theory.

The basic idea of cryptography is to camouflage confidential information. A cryptosystem completes the following disguise: a user (encryptor) transforms (encryption transformation) the confidential information (clear text) that needs to be disguised to obtain another representation (ciphertext) which seems to be irrelevant to the original information [5]. If the legitimate user (receiver) obtains the disguised information, he can restore the original confidential information (decryption transformation) from the information, if illegal users (password analysts) try to get the original confidential information from the disguised information, either such analysis is impossible at all, or the cost is too large to be carried out. At present, the mature encryption methods include DES encryption algorithm, IDEA encryption algorithm, ECC encryption algorithm, RSA encryption algorithm, etc. from the current domestic and foreign research status, it is necessary to achieve the ideal goal of high efficiency and security in information transmission, and the development of encryption technology to the cross use of RSA and AES is inevitable. However, different encryption algorithms have different defects, such as RSA has a slow encryption speed and low security of AES encryption results.

At present, reference [6] proposed a data encryption method based on adversarial neural network. By analyzing the idea of counterattack neural network and introducing the counterattack game theory of cryptography, a counterattack neural network encryption method based on selective ciphertext attack is proposed. By introducing the attacker of selective ciphertext attack, the existing encryption algorithm of neural network is improved to complete the data encryption processing. Reference [7] proposed a data encryption method based on cloud computing. This method firstly analyzed the traditional symmetric encryption algorithms DES and AES, and compared their advantages and disadvantages in the cloud computing model. Then, combined with Hadoop distributed computing framework, an improved DAES hybrid encryption algorithm is proposed. This algorithm can effectively improve the security by mixed encryption of plaintext partition and adding random disturbance information.

In order to solve the problems existing in traditional encryption algorithm, a hybrid encryption method is proposed. The principle of this method combines source encryption with line encryption. The specific method is: users encrypt plaintext, and encrypted ciphertext directly enter the line secret machine, perform a second encryption. In order to improve the mixed encryption effect of cross border e-commerce

information and ensure the security of cross border e-commerce transaction information, B+ search tree algorithm is introduced. B+ tree is a variant tree of B-tree which is required by file system. Usually, there are two head pointers on B+ tree, one pointing to root node and one pointing to leaf node with the smallest keyword. With the application of B+ search tree algorithm, the operation security of cross border e-commerce transaction information is improved to the lowest extent by mixing two or more encryption algorithms.

2 Design of Hybrid Encryption Method for Cross Border E-commerce Transaction Information

2.1 Using B+ Search Tree Algorithm to Retrieve E-commerce Transaction Data

In the basic B-tree, the keywords are distributed in the whole B-tree, and the keywords that appear in the internal nodes no longer appear in the leaf nodes, so that the order chain cannot connect all the keywords in the tree. B+ tree has changed this point, that is, all keywords in the tree are inserted on the leaf node from left to right in increasing order, and connected with pointers. In B+ tree, data pointers are only stored in the leaf node of the tree. Therefore, the structure of leaf node is different from that of internal node. If the search field is a keyword, the leaf node has an entry and a pointer to the record for the value of each search field. For non key search fields, the pointer points to a block in the add-on level, which stores the record pointer to the data file [8]. The structure of B+ search tree is shown in Fig. 1.

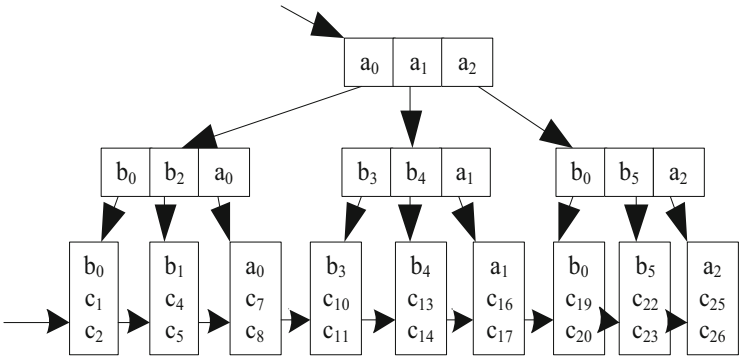


Fig. 1. B+ search tree structure

It can be seen from Fig. 1 that B+ search tree is a three-layer structure from top to bottom, and all the key codes appear on leaf nodes. The key codes in nodes of each layer above are copies of the largest key codes in corresponding nodes of the next layer. Since the construction of B+ tree is bottom-up, M limits the size of nodes and

copies the maximum key code of each node to the node of the previous layer from bottom to top.

In order to enable searchers to quickly find the transaction identifiers of ciphertext documents related to trap door transactions on the block, the data owner stores the transaction identifiers related to ciphertext transactions in the leaf nodes of B+ tree, where the structure of the nodes is shown in formula 1.

$$u = (N, D, P_1, P_r, TXid) \tag{1}$$

where, N is the node number in the tree index structure, D is the m dimensional vector composed of m keywords of each document, P_1 and P_r are the left and right pointers of node u respectively. If u is the leaf node of the index tree, the transaction identifier txid of the ciphertext document is stored in the leaf node, and if u is the internal node, the calculation of node vector D is shown in Eq. 2.

$$D[j] = \max\{u.P_1 \rightarrow D[j], u.P_r \rightarrow D[j]\} \tag{2}$$

The process of inserting nodes into B+ tree is the process of building ciphertext transaction index. In the actual cross border e-commerce transaction information retrieval process, we need to search the B+ tree node and find keywords in the B+ node on the cross border e-commerce platform to get the corresponding transaction information retrieval results [9]. Suppose that the B+ tree of order m contains N keywords, and the analysis shows that there are at least $2 \times \left\lceil n^{\frac{2}{m}} \right\rceil^{k-1}$ nodes in layer k. If the B+ tree is inserted, it will split. Let L be the number of internal nodes. When all internal nodes except the root contain $\left\lceil n^{\frac{2}{m}} \right\rceil^{-1}$ keywords, the B+ tree contains the least number of total keywords:

$$N \geq 1 + L\left(n^{\frac{2}{m}} - 1\right) \tag{3}$$

That is to say, in the worst case, each inserted node of L is split, that is, L is split, then the average number of split nodes for each inserted key is:

$$S = \frac{K}{N} \tag{4}$$

In the B+ search tree algorithm, through the cross border e-commerce trading platform of each node location data search, get the final search results.

2.2 Data Acquisition and Processing of E-commerce Transaction Information

In the process of data collection, the first step is to simulate the operation of the browser on the page, and then analyze the structure of the page through the given URL. For ordinary pages, the basic Http Client method is used to obtain them. For special pages,

it is necessary to further determine whether they are dynamically loaded pages or pages that need further interaction to obtain data [10]. For pages with dynamic secondary loading information, Htmlunit provides Web Client.get Options().set Java Script Enabled() method to parse JavaScript scripts. For Ajax, the web client. Set Ajax controller () method is also provided to support Ajax. Therefore, htmlunit can directly parse the dynamic secondary loading information page. The transaction statement set can be obtained from the transaction web page data after preprocessing, and these transaction statement sets still contain a lot of noise, such as non transaction statement, invalid transaction, etc. if the transaction statement is analyzed and extracted directly, the results may deviate from the actual situation, or even draw wrong conclusions. Therefore, we need to filter and clean the product transaction statement set again. In the actual processing process, the noise in the product transaction sentence set is mainly manifested in the following aspects: the non transaction noise such as characters irrelevant to the transaction sentence and explanatory text, which will increase the time consumption of further analysis of the transaction sentence, and also cause interference to the syntactic analysis and opinion extraction of the transaction sentence; Automatic transactions of e-commerce platform, such as “default praise” transactions, have no significance for the extraction and analysis of the whole transaction view; In order to obtain benefits, some businesses or competitors mislead consumers by publishing statements to promote or slander a certain brand product, or even asking the Internet water army to publish false transactions, which will cause interference to the analysis results of the overall view of the transaction and need to be filtered out; For non trading statements in Product Trading Web data, direct filtering method can be adopted to extract trading statements. For noise trading in trading statement set, for unrelated product trading statements and non trading statements, firstly, the garbage trading set is obtained by manually marking training set, and then the machine learning model is established by logistic regression to identify these two types of invalid transactions; For the deceptive trading information such as defamation, promotion and interference, the repetitive trading information is identified by machine learning model, which takes the repetitive trading data statements as the positive training set.

2.3 Clustering Cross Border E-commerce Transaction Information

Clustering is to divide a physical or abstract data set into several classes. The data in each class has great similarity, and there is little similarity or dissimilarity between classes. Its analysis basis is the similarity calculation between data. By clustering the cross border e-commerce transaction information, it is convenient for the hybrid encryption algorithm to process the same type of data, so as to improve the encryption effect. The clustering process of cross border e-commerce transaction information is shown in Fig. 2.

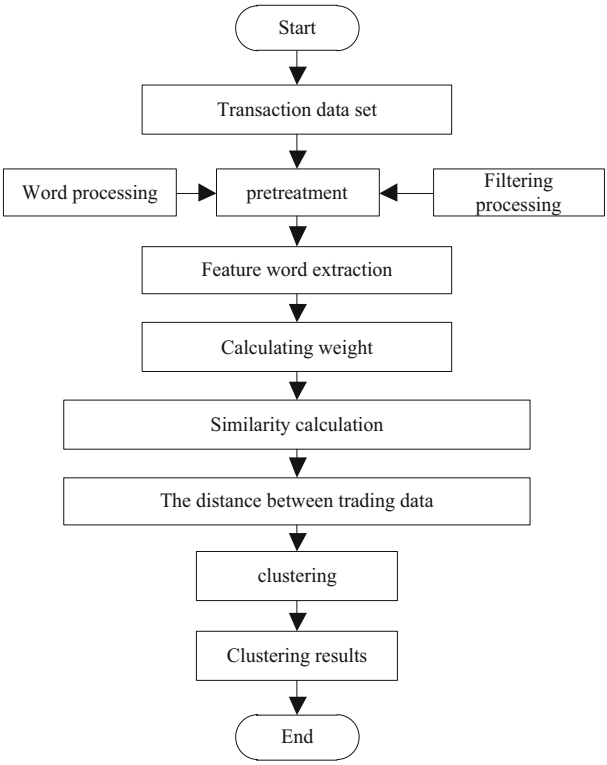


Fig. 2. Cross border e-commerce transaction information clustering flow chart

In clustering analysis of product transaction data statements, it is necessary to calculate the similarity of transaction data statements, and classify the statements with similar transaction contents into one category. When the transaction data is vectorized, in order to reduce the dimension of the constructed sentence vector, all the words in the sentence can not be expressed in the vector. It is necessary to extract the words that can represent the content and attributes of the transaction data in the transaction sentence, that is, the feature words, and extract them to form the vector representation of the transaction sentence [11]. Transaction data vectorization is to abstract each feature word of transaction data into a component of sentence vector. For the convenience of description, the transaction data to be classified is defined as:

$$D = \{S_k, K = 1, 2, 3 \cdots\} \tag{5}$$

After S_k is processed by word segmentation, pronoun removal and auxiliary word removal, the remaining words are used as feature words to construct the vector model of the sentence, and the set of feature words of S_k is represented as S_{kw}, which is the basis of constructing the similarity calculation model. After the feature word set representation of the sentence is obtained, the weight of each feature word in the set in the

transaction data is calculated, and the weight value of each feature word is composed of the following vectors:

$$V_s = (v_1, v_2, \cdots, v_k) \tag{6}$$

v_i represents the weight of the corresponding feature word w_i in the transaction data, which constitutes a k-dimensional space vector and realizes the vectorization of the transaction data.

In order to meet the requirements of processing time when processing text big data, the weight value of each feature word in the transaction data vector is calculated [12]. Usually, the importance of a feature word increases with the frequency of its appearance in the document, but decreases with the frequency of its appearance in the corpus. The word frequency TF represents the frequency of feature word w_i appearing in transaction data D, and the importance of w_i to document D is expressed as follows:

$$TF = \frac{N_{w_i}}{N_{Dw_i}} \tag{7}$$

where N_{w_i} is the number of times that feature word w_i appears in document D, and N_{Dw_i} is the total number of words in document D. In addition, the inverse document frequency IDF represents the number of documents containing the feature word w_i in the corpus, and the value of IDF is calculated by using the following formula:

$$IDF = \lg \frac{N_D}{N_{w_i D}} \tag{8}$$

where N_{w_i} is the number of times that feature word w_i appears in document D, and N_{Dw_i} is the total number of words in document D. In addition, the inverse document frequency IDF represents the number of documents containing the feature word w_i in the corpus, and the value of IDF is calculated by using the following formula:

$$v_i = TF \times IDF \tag{9}$$

In order to improve the efficiency of feature word weight calculation, the map reduce framework is used to make word statistics on the transaction statements of each storage node, and the statistical results are summarized. When calculating TF and IDF values in TF-IDF algorithm, there is no need to repeat the statistical operation, which saves the statistical time and improves the efficiency of the algorithm. In the cross border e-commerce transaction information, select the appropriate clustering center, and calculate the similarity of transaction information [13]. The weight of the feature words of two sentences in the transaction data is used to form the vector representation of the sentence, that is, the feature vector of the sentence is obtained, and then the cosine value of the angle between the feature vectors is used as the similarity value of the sentence:

$$Sim(S_1, S_2) = \frac{\sum_{i=1}^{n} \phi_i \cdot \psi_i}{\sqrt{\sum_{i=1}^{n} \phi_i^2} \cdot \sqrt{\sum_{i=1}^{n} \psi_i^2}} \tag{10}$$

ϕ_i and ψ_i represent the eigenvector components of sentence S_1 and S_2 respectively. Based on the above operations, the number of cluster centers K is initialized by K-means algorithm, and K transaction statements are randomly selected as cluster centers. The distance between each transaction information and K cluster centers is calculated respectively, and each transaction is allocated to the cluster with the nearest cluster center, and the cluster center of each family is recalculated. Finally, determine whether the new cluster center and the original cluster center are less than the threshold value. If it is less than the threshold, the cluster results will be output directly, otherwise, the above steps need to be performed again. The final result of clustering processing of cross border e-commerce transaction information is shown in Fig. 3.

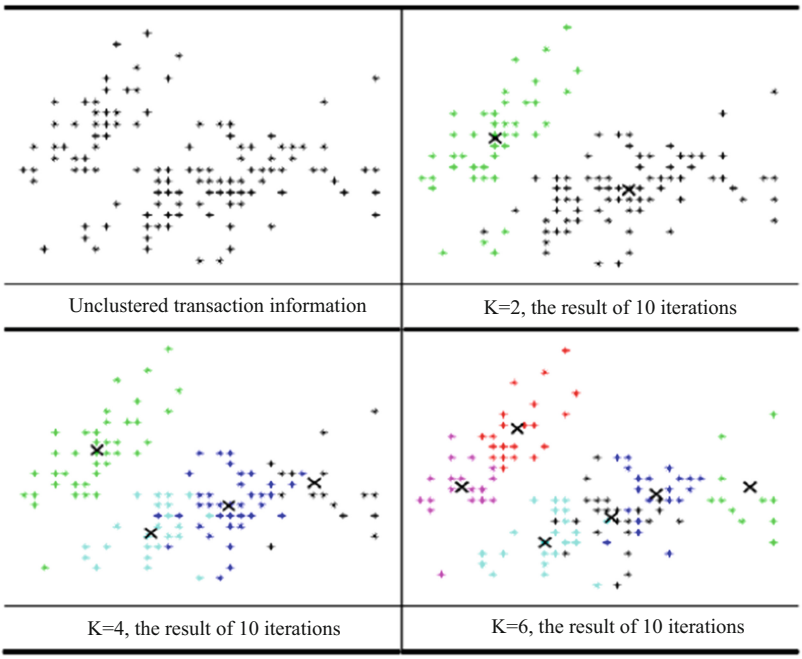


Fig. 3. Clustering effect of e-commerce transaction data under different K values

2.4 Select Hybrid Encryption Algorithm Type

In accordance with the principles of accuracy, simplicity, efficiency and practicability, the type of hybrid encryption algorithm is selected. This paper compares the

performance of encryption algorithm from two aspects of security and encryption speed, and the comparison results of encryption algorithm performance are shown in Table 1.

Table 1. Performance comparison of encryption algorithms

Encryption algorithm type	How long does it take to decode the key/h	Key length/bit
AES	108	768
DES	104	512
RSA	204	768
MD5	1011	21000
IDEA	1020	2048
ECC	1078	1024

As can be seen from Table 1, compared with other asymmetric cryptography technologies, IDEA and ECC cryptography technologies have absolute advantages in anti attack and cracking performance. Through continuous testing, scientists have come to the conclusion that if IDEA and ECC want to decode, the difficulty is far greater than that of algorithms such as RSA, and they are not on the same level at all. If ECC and RSA are in the same computing conditions, RSA algorithm can reduce the length of public key to improve the encryption efficiency, and improve the speed of digital signature and authentication. However, in the private key processing level, elliptic curve algorithm has much higher data processing efficiency than the other two algorithms. And its key generation speed is much faster than the other two. Therefore, if these algorithms are in a peer-to-peer computing environment, the overall resource consumption and processing efficiency of ECC algorithm are much better. To sum up, IDEA encryption algorithm and ECC encryption algorithm are selected as hybrid algorithms.

IDEA algorithm is a symmetric key block cipher system, its plaintext and ciphertext are 64 bits, and the key length is 128 bits. The data is encrypted in 64bits packets. The encryption process is to iterate the input 64bits plaintext for 8 rounds, and the resulting iteration result is transformed into the final output 64bits ciphertext group. ECC encryption algorithm is also known as elliptic curve encryption algorithm. The order of the curve is defined as the number of all points on the elliptic curve, denoted as E, which satisfies the following relationship:

$$p + 1 - 2\sqrt{p} \leq E \leq p + 1 + 2\sqrt{p} \tag{11}$$

The finiteness of points and the uncertainty of the number of points on elliptic curve group are good attributes for encryption, because these curves only contain some discrete points, and the attacker does not know how to apply the geometric relationship. Suppose that a point P on an elliptic curve satisfies the minimum positive integer n of number multiplied by $n_P = 0$, which is called the order of point P. The implementation of elliptic curve cryptosystem is determined by the domain parameters of elliptic curve, which include the base domain of elliptic curve, curve equation, base

point of curve and order of base point. The parameters of elliptic curve domain are public and shared by both sides of communication. Randomly select an integer d in the interval $[1, n-1]$ and calculate the formula as follows:

$$Q = dP \tag{12}$$

where d is the private key and Q is the public key. The following nodes are specific to the body area network application, node A represents the collection node, and node B represents the sink node. In the encryption process, when node A sends physiological information to node B, node A encodes the physiological information M to be transmitted to a point m on $E_p(a, b)$. Node A looks up node B's public key Q_B and public information base point P, and transmits encrypted data C_1 and C_2 to node B.

2.5 Realize Cross Border E-commerce Transaction Information Hybrid Encryption

Taking node B as the collection node to send physiological information to sink node A as an example, in the previous discussion, the key encapsulation mechanism will include three sub processes, namely, the generation of A and B public keys, the key encapsulation of B and the key unsealing of A. The core idea of the algorithm is that A and B use the same shared secret key. The specific idea is that A uses its own private key and B's public key to carry out the corresponding operation. At the same time, node B uses B's private key and A's public key to carry out the same operation. On the basis of elliptic curve encryption, the key encapsulation of hybrid encryption system is shown in the figure below (Fig. 4).

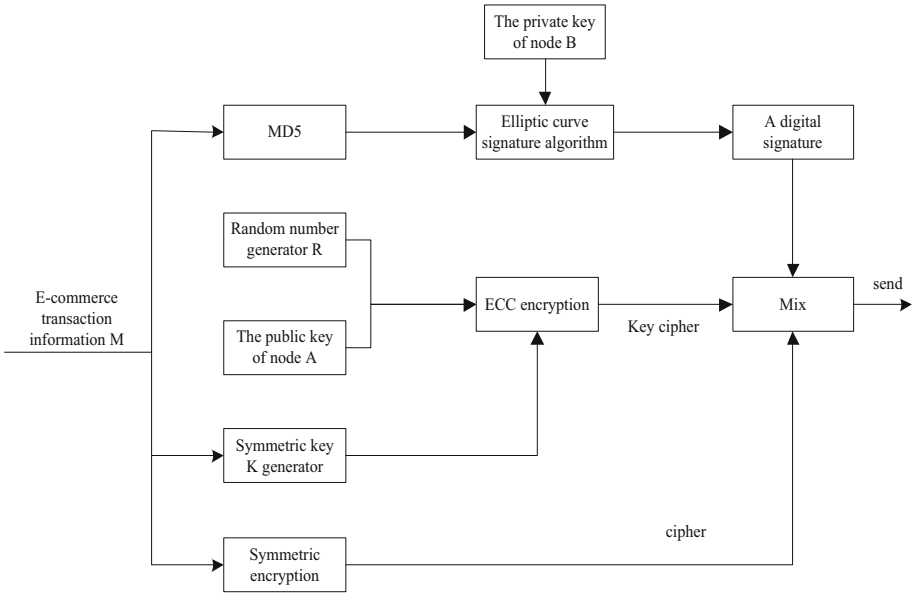


Fig. 4. Block diagram of hybrid encryption key encapsulation

Generate Key and Private Key

Through the combination of idea and ECC algorithm, the following mixed encryption expression is formed

$$\begin{cases} x_{n+1} = ax_n(1 - x_n) \\ y_{n+1} = by_n(1 - y_n) \end{cases} \tag{13}$$

where, x_n and y_n are the input items of cross border e-commerce transaction information, x_{n+1} and y_{n+1} are the final encryption results, and a and b are constant coefficients. In the process of generating ECC private key, the first step is to input the initial value $(X0, Y0)$, the number of iterations n, and the parameters a and b; The input parameters are used as the input parameters of the hybrid encryption method for iteration until the required number of iterations n is reached, and the final iteration result is returned. Calculate the result of $X \times Y$ is denoted as T_1, and the integer of T_1 is denoted as T; If T is less than the multiple of ECC's base point, then T is assigned to key as ECC's private key; Otherwise, return to the first step.

Key Management and Distribution

The key distribution includes the distribution of public key and secret key. The public key distribution is also the problem of how to obtain the public key of the other party in the system of public key cryptosystem. First, the key and public key are obtained by using the key generation software. The private key is in the local file and cannot be passed out. As for public key is public password, it can be known to others. Then the central computer needs to save the KU receiving of each node in the local special file system. In this component, the data encryption transmission process is: in the initial stage, the background center computer generates an encryption key. If it is called DEKEY, then a key for signature is generated. If it is called MKEY, both keys need to be saved. Then, we need to encrypt two keys by using elliptic curve algorithm, and the encrypted key is. Then, the encrypted DEKEY and MKEY are transmitted to the front desk. The client decrypts the data to get key and MKEY by using the private DEKEY generated by elliptic curve after receiving the file, and saves the obtained file in the local system.

Key Exchange in Hybrid Encryption

The key exchange method with the ability of confidentiality and authentication is adopted. The method is assumed to be carried out when the public key of both parties is consistent with each other. In fact, the certification authority now guarantees the completion of this part of the work. The confidentiality and identification are realized through two repeated verification of A and B parties. Because of the universality of encryption of common key algorithm key with public key algorithm, the scheme has a wide range of applications. A encrypts a message sent to B with the public key of B, which contains a random identifier ID_A generated by A, and B sends a message encrypted by mixed encryption method to A, which contains identifier ID_B generated by identifier ID_A and B of A. A returns a ID_B encrypted with the public key of B to

make B sure the other party is A, A selects a secret key K and sends the program parameter represented by formula 14 to B.

$$M = (E_{KP_b}(E_{KP_a}(K))) \tag{14}$$

where (E_{KP_a}, E_{KP_b}) generates a public and private key pair for A. Encryption with B's public key ensures that only B can interpret it; Encryption with the private key of A ensures that only A can send it. After receiving it, B side recovers the secret key K, and realizes confidentiality and authentication through two repeated verifications of A and B.

Cross Border E-commerce Transaction Information Mixed Encryption Transmission

The hybrid cryptographic communication process mainly involves the operation of the sender and the receiver, in which the sender's operation is regarded as the encryption process and the receiver's operation as the decryption process. The generated key and plaintext are digitally encapsulated, and the information is transmitted through the communication transmission channel. After receiving the data, the receiver can decrypt the key and ciphertext through digital signature verification.

3 Experimental Analysis of Encryption Performance Test

In order to test the encryption performance of the hybrid encryption method of cross-border e-commerce transaction information based on B+ search tree algorithm, the performance test experiment is designed, and the operational advantages of the design method are reflected through quantitative comparison with different methods.

3.1 Development Tool and Test Environment of Encryption Method

The experiment of hybrid encryption algorithm is carried out on the laboratory Hadoop experimental platform. The experimental platform consists of six computers in the laboratory. According to the structure requirements of Hadoop platform, one of the six computers acts as the namenode server, which is responsible for the scheduling control of the whole system. The other five computers are used as storage nodes and computing nodes. Due to the limitation of computers owned by the laboratory, the configuration of these five computers is not the same, and the purchase age is also different. In addition, during the experiment, these five computers were added to Hadoop cloud computing platform. Now the configuration of these six computers is briefly introduced, as shown in Table 2.

Table 2. Configuration of computers used in the experiment

Name	CPU	Frequency	Memory	Hard disk
Cloud2	Pentium 4	3.0G	512 MB	80G
Cloud3	Pentium 4	3.0G	512 MB	80G
Cloud4	Pentium 4	3.0G	512 MB	80G
Nodel	IS-2320	3.0G	3G	150G
Node2	IS-2320	3.0G	3G	150G
M290	IS-2320	3.0G	3G	150G

It can be seen from Table 2 that among the six computers, the computing power and storage capacity of three computers are better than those of the other three computers. In this case, according to the experimental requirements, the operator selects the computer with higher computing power and storage capacity as the computing node and storage node. This design also meets the requirements of high computing power of hybrid encryption algorithm experiment. In addition to the hardware requirements, the experimental platform also has certain software requirements. The Hadoop cloud computing platform composed of six computers in the laboratory uses Ubuntu 10.10 as the operating system and Hadoop 0.20.203 as the Hadoop system version. In addition, because the processing object of the encryption method exists in the form of document, and the designed encryption method applies B+ search tree algorithm, it is necessary to embed multiple processing programs in the experimental environment. For example, Weblogic 10 is used as the development server. The WebLogic Server configures the JSP container by configuring the weblogic.xml file. The weblogic.xml file can be used in the web of the configured web application_ Inf directory. Generally speaking, it is not necessary to modify the Weblogic. XML file manually for developing and deploying web applications. When deploying the application again, you can configure it in the console. Select the deployment option in the console and click webapplication to configure the web application. Then the corresponding configuration file can be generated in the system. Developers can configure different information in development and production environments.

3.2 Prepare Cross Border E-commerce Transaction Data Samples

The cross border e-commerce transaction data encrypted in the experiment mainly comes from the cross border e-commerce transaction platform. In this experiment, the home decoration design e-commerce platform is selected to provide transaction data samples for the experiment. The operation of the platform is shown in Fig. 5.

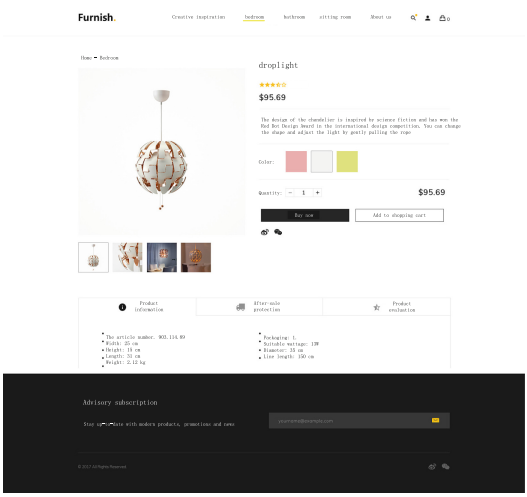


Fig. 5. Cross border e-commerce transaction interface

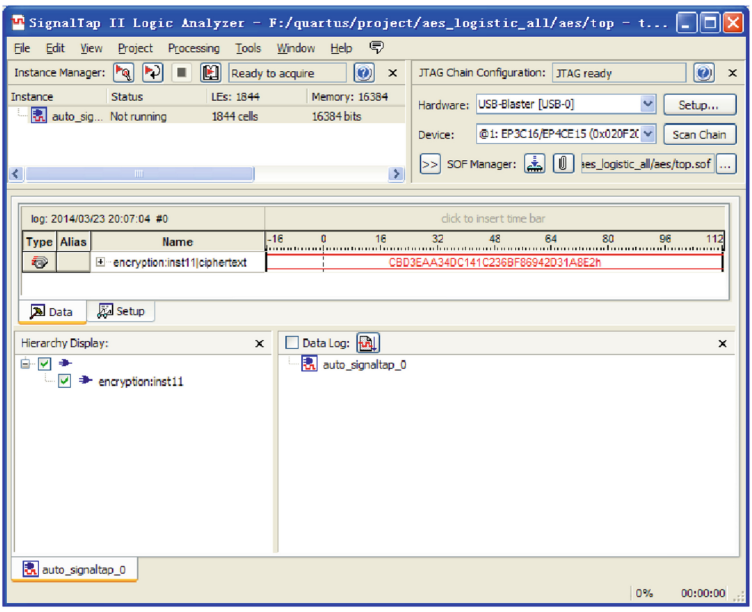
All transaction data in the trading platform are collected as data samples during the half year from October 2020 to March 2021, with a total of 24.17 GB of transaction data.

3.3 Set up Experimental Comparison Items and Test Indexes

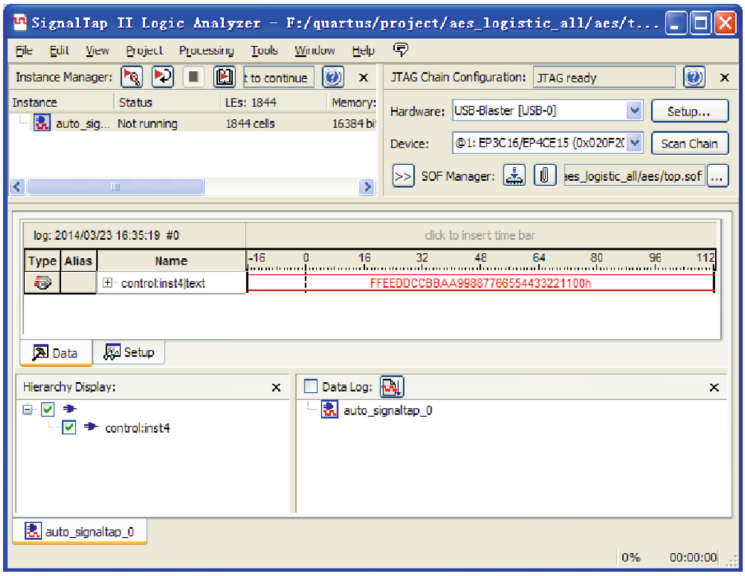
In order to reflect the performance of the design encryption method, the encryption method based on the adversarial neural network and the encryption method based on cloud computing are set as the two contrast methods of the experiment, and the two contrast methods are imported into the experimental development and operation environment in the same way. In the experiment, the cross-border e-commerce transaction data processed by the three encryption methods are the same, so as to ensure the uniqueness of the experimental variable. The security of the encryption result is set as the test index of the encryption performance, which consists of two parts, namely the key cracking time and the data error amount of the decryption result. The longer the key cracking time, the higher the encryption effect, while the more the data error amount of the decryption result, the lower the security of the encryption method.

3.4 Describe the Experimental Process of Encryption Performance Test

In order to effectively simulate the actual cross border e-commerce trading platform environment, the attack program is used to attack the transaction data, and the attack frequency and intensity are controlled. According to the attack settings, the experimental groups are divided, and the final comprehensive test results are obtained by averaging multiple experiments, so as to enhance the credibility of the experimental conclusions. Through the operation of the three encryption methods, the corresponding encryption results are obtained. The output results of the designed hybrid encryption method are shown in Fig. 6.



(a)Ciphertext results obtained by hybrid encryption



(b)Plaintext sequence received by receiver

Fig. 6. Cross border e-commerce transaction information mixed encryption results

3.5 Analysis of Test Results

Through the statistics and analysis of relevant data, the quantitative test results of key cracking time are obtained, as shown in Table 3.

Table 3. Statistics of key cracking time test(h)

Experimental group	Encryption method based on adversarial neural network	Encryption method based on cloud computing	Design encryption method
1	16.4	25.4	35.4
2	19.8	22.8	42.6
3	21.4	26.5	38.9
4	18.6	27.1	34.1
5	20.4	23.5	33.7
6	17.5	22.7	45.1
7	14.3	24.4	37.4
8	18.4	26.3	42.2

It can be seen from Table 3 that the average key cracking time of the three encryption methods is 18.35 h, 24.84 h and 38.68 h respectively, which shows that the key cracking time of the encryption method is longer.

In addition, the results of the three encryption methods are decrypted, and the statistical results of the amount of data errors are obtained under different attack environments, as shown in Table 4:

Table 4. Statistics of decryption data error

Experimental group	Encryption method based on adversarial neural network		Encryption method based on cloud computing		Design encryption method	
	Data loss/MB	Amount of error data/MB	Data loss/MB	Amount of error data/MB	Data loss/MB	Amount of error data/MB
1	1.14	1.25	0.56	0.56	0.14	0.04
2	1.28	1.31	0.52	0.48	0.07	0.05
3	1.06	1.45	0.78	0.42	0.08	0.02
4	1.26	1.52	0.69	0.63	0.13	0.04
5	1.31	1.40	0.61	0.48	0.11	0.11
6	1.36	1.26	0.72	0.44	0.05	0.06
7	1.29	1.31	0.59	0.61	0.06	0.03
8	1.44	1.09	0.49	0.75	0.10	0.07

Through the statistics of the data in Table 4, we can see that the data errors of the three encryption methods are 2.59 MB, 1.17 MB and 0.15 MB respectively. To sum up, from the two aspects of the key cracking time and the amount of decrypted data errors, the security of the design encryption method is higher.

4 Concluding Remarks

As a new data encryption algorithm, hybrid encryption algorithm will be more effective, secure and flexible than the past simple encryption/decryption algorithm. The hybrid encryption method combining IDEA and ECC not only solves the difficulty of key distribution, but also solves the speed and efficiency of encryption and decryption. Undoubtedly, it is a better and feasible method to solve the problem of information security. According to the diversity of existing encryption algorithms, hybrid encryption/decryption algorithm has a better development prospect.

Fund Projects. 1. Key scientific research platforms and projects of ordinary universities in Guangdong Province in 2020-Research on cross-border E-commerce blockchain information security technology based on B+ search tree algorithm (Item No.: 2020ZDZX3103)

2. "Innovation Research on Cross-border E-commerce Shopping Guide Platform Based on Big Data and AI Technology", Funded by Ministry of Education Humanities and Social Sciences Research and Planning Fund (18YJAZH042).

References

1. Zhang, B., Tan, R., Lin, C.J.: Forecasting of e-commerce transaction volume using a hybrid of extreme learning machine and improved moth-flame optimization algorithm. Appl. Intell. **12**(05), 1–14 (2020)
2. Liu, S., Liu, X., Yuan, J., et al.: Multidimensional information encryption and storage: when the input is light. Research **2021**(01), 1–17 (2021)
3. Borrego, C., Amadeo, M., Molinaro, A., et al.: Privacy-preserving forwarding using homomorphic encryption for information-centric wireless ad hoc networks. IEEE Commun. Lett. **23**(10), 1708–1711 (2019)
4. Li, Z., Yang, X., Shen, K., et al.: Information encryption communication system based on the adversarial networks Foundation. Neurocomputing **41**(05), 347–357 (2020)
5. Ma, H., Zhang, Z.: A new private information encryption method in Internet of Things under cloud computing environment. Wirel. Commun. Mob. Comput. **2020**(6), 1–9 (2020)
6. Zhuang, W.: Research on data encryption technology based on adversarial neural network. Comput. Eng. Appl. **49**(4), 5–15 (2019)
7. Zhan, F., Zhang, S.R.: Research on hybrid encryption DAES algorithm based on cloud computing. Electron. Des. Eng. **25**(3), 185–189 (2017)
8. Salameh, J., Al-Tarawneh, M.S.: A Secure exchange technique for secret information and encryption key using hybrid system. Int. J. Commun. Antenna Propag. **9**(1), 19–26 (2019)
9. Lai, J., Cai, S.: Design of Sino-Japanese cross border e-commerce platform based on FPGA and data mining. Microprocess. Microsyst. **80**(07), 103360–103372 (2020)
10. Wang, S.Y., Wu, X.F., Hu, S.G., et al.: A hybrid encryption algorithm based on Logistic chaotic equation and ECC. Mod. Inf. Technol. **2**(2), 103–104 (2018)

11. Liu, Y.C., Wang, J., Qu, Q.F.: Text information hiding technique by carrier of song poetry based on hybrid encryption. Comput. Technol. Dev. **28**(01), 138–143 (2018)
12. Chen, Y.W., Liu, Y.L., Ma, L.T., et al.: Research on improvement of AES and ECC algorithm and hybrid encryption for substation. Foreign Electron. Meas. Technol. **39**(10), 68–73 (2020)
13. Liu, Q.Y., Chen, L., Liu, L.: A hybrid encrypted file protection system based on hardware fingerprint. J. Shandong Agric. Eng. Univ. **36**(01), 53–56 (2019)