Data Security Transmission Algorithm of Remote Demonstration System Based on Internet of Things

Yong-sheng Zong[1,2(✉)] and Guo-yan Huang[1]

[1] College of Information Science and Engineering, Yanshan University, Qinhuangdao 066004, China
[2] Qinhuangdao Vocational and Technical College, Qinhuangdao 066100, China

Abstract. Traditional remote demonstration data transmission methods neglect the evaluation of data trust, which leads to the problem of high packet loss rate in data transmission. In order to solve this problem and optimize the security of remote demonstration, a secure data transmission algorithm of remote demonstration system based on Internet of Things is proposed. Through four parts of system data fusion processing, system data compression, data trust evaluation and data encryption transmission, the design process of remote demonstration system data security transmission algorithm based on the Internet of Things is completed. The example test link is constructed, and the application effect of the Internet of Things algorithm is confirmed through three groups of experiments with different indexes. In the future use of the remote demonstration system, this algorithm can be used to realize the high security transmission of data.

Keywords: Internet of Things technology · Remote demonstration system · Data encryption · Data transmission

1 Introduction

With the development of Internet and industrial manufacturing level, more and more industrial data are stored in enterprise database, but due to the lack of effective data analysis and management tools, data can not fully play the function of equipment application guidance, and only through remote demonstration system can this function be realized. The current mainstream of remote monitoring technology is the application of Internet technology, supporting TGP, IP protocol and WWW technical specifications, well-organized software, enabling staff to access network servers quickly to all their access information and timely response [1, 2]. In the future, the development of embedded system will be more and more rapid and mature. New technology will be applied to remote demo system in the future, which is a demo system design. Embedded demo system can realize information to improve the positioning of server performance, so that each device can have Internet access and service functions, that is, each device can serve independently, thus greatly improving the quality of service range.

S. Liu and X. Ma (Eds.): ADHIP 2021, LNICST 417, pp. 239–253, 2022.
https://doi.org/10.1007/978-3-030-94554-1_20

At present, the use of the system gradually expanded the scope of the system's data gradually increased. Massive data, which emerged in recent years with the development of information technology, especially Internet technology, is mainly used to describe huge and unprecedented data, such as various environmental and cultural data information such as spatial data, report statistics, text, voice, image, hypertext, etc. Now, many enterprises, companies are involved in the operation of mass data processing, such as water conservancy departments, meteorological departments, such as processing data are very large. Because the mass data is very large, the reasonable compression and storage of the mass data become the supporting technology to solve the mass information storage and transmission. Because of the limitation of the technology and the complexity of the mass data, the efficiency and reliability of the remote demonstration system is low. In this paper, these problems are analyzed and improved.

In the past research, many remote demonstration system data security transfer algorithms have been proposed [3, 4], but there are some problems in the use of physical network technology to optimize it. The resolution of the Internet of Things has attracted great attention all over the world, and the research on the Internet of Things is becoming more and more in-depth. According to the definition of the International Telecommunication Union, the Internet of Things mainly deals with the interconnection of goods to goods, people to goods and people to people. The Internet of Things is a new type of real-time interactive system between virtual network and real world, which is characterized by ubiquitous data perception, wireless information transmission and intelligent information processing. The extensive application of the Internet of Things can provide convenience and bring social benefits for people in their lives and work. However, because a lot of information transmission in the Internet of Things relies on wireless networks, and a lot of devices are exposed to the public, information is vulnerable to theft and attack, and devices are vulnerable to damage, the security risks brought by the Internet of Things have been paid more and more attention. In this study, the application of this technology to optimize the traditional algorithm, and strive to improve the performance of the algorithm on the basis of the traditional algorithm.

2 Design of Data Security Transmission Algorithm for Remote Demonstration System

In this study, the Internet of things technology is applied to the design of remote demonstration system data security transmission algorithm, and the design process of system data security transmission algorithm is set as shown in Fig. 1:

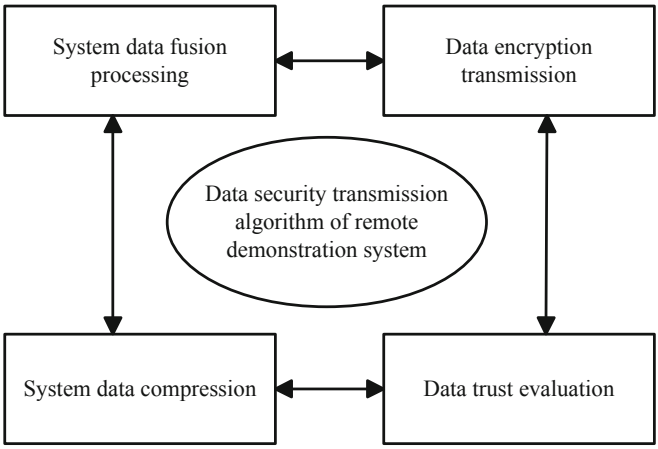

Fig. 1. Design flow of system data security transmission algorithm

In this design, the main work content is as follows:

(1) Describe the current research status of data security transmission algorithms, point out the existing problems and defects, and introduce the significance of research on privacy protection.

(2) This paper introduces the basic concepts and architecture of the Internet of Things, describes the role of the Internet of Things in data transmission and the security goal of data transmission, and finally expounds the trust evaluation theory and data encryption used in this paper in detail.

(3) This paper analyzes the existing problems in evidence merging, and proposes a new recommended merging rule, which can resist the safe data transmission algorithm of malicious defamation, and proves the performance of the algorithm through experiments.

2.1 System Data Fusion Processing

The basic idea of data fusion is that the upper nodes analyze the data transmitted by the lower nodes, filter, compress, remove the redundant information, and only send useful information to the upper nodes. This saves energy and prolongs the life of the node [5, 6]. The IOT awareness layer is made up of a lot of nodes distributed everywhere. If the nodes are densely distributed, the data between different nodes may be overlapped. If the nodes transmit all the data to the base station, it will first bring a large amount of data transmission consumption. Secondly, too much data may lead to data collision and affect the accuracy of the data. Finally, these data will be transmitted to other nodes, bringing more energy consumption. How to make full use of limited resources is the focus of wireless network research.

Through analyzing the noise characteristics of the system module, the measurement of the target parameters of the system module is described in the design of data fusion model by the following models:

$$y_i(s) = x(s) + \varepsilon_i(s) \tag{1}$$

In the above formula, $x(s)$ is used to represent the measured value of the system module during i-th measurement. $\varepsilon_i(s)$ represents the comprehensive noise generated by the system module in the i-th measurement, and meets the requirements of $C[\varepsilon_i] = 0$ and $H[\varepsilon_i] = W_i^2$. The comprehensive noise includes the noise of the system module itself and the external noise of the environment in which the system module is located. $y_i(s)$ is the overall distribution, and it is considered in the above formula, The integrated noise between the system modules is completely independent.

Set n systems module to measure the same target, the data distribution of the i-th system module and the j-th system module is V_i, V_j. V_i, V_j obeys Gauss distribution, and its PDF curve is taken as the characteristic function of the system module, denoted as $r(V_i)$, $r(V_j)$, V_i and V_j, which are the first observation values of V_i and V_j respectively.

In order to reflect the deviation between v_i and v_j, the concept of relative distance is introduced:

$$d_{ij} = abs\left|v_i - v_j\right| \tag{2}$$

Where, d_{ij} is the distance. From the expression d_{ij}, the larger d_{ij} is, the greater the difference between v_i and v_j, the lower the degree of mutual support between v_i and v_j. Therefore, a function f related to e is introduced to represent the mutual support relationship between v_i and v_j. q_{ij} itself shall meet the following two conditions:

(1) q_{ij} should be inversely proportional to the relative distance d_{ij};

(2) The value range of q_{ij} should be limited between [0, 1], that is, $q_{ij} \in [0, 1]$.

The support function obtained by the above method is simple in form and easy to implement. In the process of using, it needs to carry out accurate calculation to ensure the effect of data compression. Suppose $U_1, U_2, ..., U_n$ homogeneous system module makes a measurement once in the measurement period t, and the sampling data matrix is obtained as follows, where $q_n(m)$ represents the m-th measurement value of node n.

$$Q = \begin{bmatrix} q_1(1) & q_1(2) & \ldots & q_1(g) \\ q_2(1) & q_2(2) & \ldots & q_2(g) \\ \ldots & \ldots & \ldots & \ldots \\ q_n(1) & q_n(1) & \ldots & q_n(g) \end{bmatrix}_{n*g} \tag{3}$$

The column data in data matrix Q is normalized and the error data is eliminated by the following formula:

$$\begin{cases} Q_i < \alpha, \text{eliminate} \\ Q_i \geq \alpha, \text{retain} \end{cases} \tag{4}$$

The optimal value of threshold α is obtained through multiple data calculations. When the data deviates from 1 to a large extent, the data is removed. Otherwise, it is retained to obtain a new column matrix, which is used to complete data fusion.

2.2 System Data Compression

Using parallel compression algorithm, the parallel compression unit of system data is designed. According to the traditional algorithm, the data parallel compression program

is divided into the following functional modules: statistics module, data segmentation module, task allocation module, probability model building module, encoder, decoder, process control module and protocol module [7]. Each module is responsible for part of the functions of the program and completes the parallel compression of massive system data. The Fig. 2 shows the data compression process.

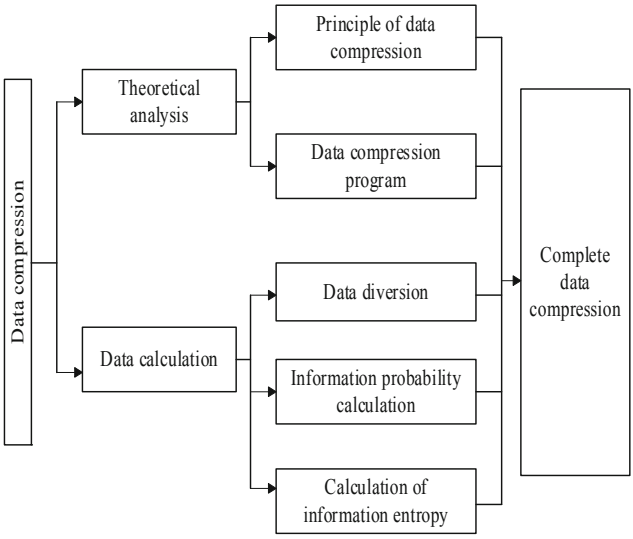

Fig. 2. Data compression process

Raw data analysis is the analysis of a large number of initial text files. Analysis needs to be done with a unicode code because it can handle both Chinese and English characters. In addition, when analyzing massive data text, there is no need to analyze the information like the header and the end of the file, just write it as it is, which is very small in proportion to the data text and is not in the scope of compressed text [8].

After analyzing the initial data stream, the frequency of the characters in the data stream should be counted. The statistical process is implemented by creating a dynamic linked list, which is used to record data and how often it occurs. As the number of characters increases, the linked list becomes larger and larger, so dynamic memory allocation techniques are used. In the statistical process, each input character also involves the data the inquiry work. To reduce the search time, the program remembers the previous character, and then when the new character is read as a memorized character, the frequency of the character is updated directly at the position specified by the memorized pointer. Otherwise, it needs to search from the beginning, find the matching character, change the character count, and if no matching character is found, reallocate the space, and insert the character into the list [9].

Probability calculation is to make statistical analysis according to the above statistical results, calculate the frequency of characters, and create a two-dimensional array to store characters and their probability. This probability will be applied to the original data

segmentation. The character probability formula is as follows:

$$P_i = \frac{F_i}{\sum_{1}^{n} F_i} \tag{5}$$

Among them, F_i refers to the frequency of the i character, n refers to the number of characters, and P_i refers to the probability of characters. In order to make the compression result more reasonable, the data is segmented reasonably. Data segmentation module is very important in the whole algorithm. It not only determines the task allocation of each processor, but also involves the problem of load balancing among processors. The quality of segmentation algorithm directly determines the efficiency of data transmission algorithm [10].

In the field of data transmission and data compression, information entropy is a concept used to measure the amount of information, which reflects the order degree of the system. The more orderly the system is, the lower its information entropy is; On the contrary, the higher the information entropy is. In the field of data compression, information entropy is used to measure the quality of a transmission algorithm and find a suitable compression codeword. For a data input stream L, its entropy is defined as follows [11]:

$$D(l) = -\sum_{i=1}^{n} l_i \log_2 l_i \tag{6}$$

If the input stream is k in length, the information for the entire input stream is:

$$J = k * D(l) \tag{7}$$

As can be seen, entropy is the measure of the amount of data flow information. Therefore, when we segment the input information stream, as long as the information of each part is equal, the length of the code word of each part after arithmetic coding is not much different, so that the final tasks of each processor are not different, and their synchronization problem is relatively easy to solve [12, 13]. Of course, the design of the algorithm not only considers the entropy, but also the number of processors. The above formula is substituted into the original data compression algorithm to process the data, and the processed data is used as the basis for subsequent calculation.

2.3 Data Trust Evaluation

In the above completed the system data preprocessing, in this link will be the trust of the data assessment, for the subsequent transmission of data security to provide a theoretical basis.

At present, the research of data trustworthiness evaluation model is based on a specific application, from their basic theory, it can be divided into two systems: Bayesian system and evidence theory system [14, 15]. This study will use the Bayesian system to complete the system of data trust evaluation. Bayesian estimation is one of the most commonly used

and effective methods in parameter estimation. Bayesian estimates treat the parameter to be estimated as a random variable that conforms to a priori probability distribution [16]. The process of observing the sample is to transform the prior probability density into the posterior probability density, and to modify the initial estimate of the parameter by the information of the sample. In Bayesian estimation, each new observation sample makes the posterior probability density function sharper, making it form the biggest spike near the real value of the parameter to be estimated [17].

The main theory of Bayesian estimation is: let the probability distribution of a and α be $f(a, \alpha)$, where $\alpha \in R$ is the unknown random variable parameter. Sample $A_1, A_2, ..., A_n$ has been given, we need to estimate the parameter α according to the above sample.

Firstly, Bayesian estimation regards the unknown parameter α as a random variable, and considers that prior to the experiment, there is α certain understanding of α, which is called prior knowledge. This kind of prior knowledge is expressed by some probability distribution of a, and its probability density function is denoted as $e(\alpha)$. This kind of probability distribution is called "prior distribution" of α. according to the above understanding of setting unknown parameter α [18].

Then, define $f(a_1, \alpha)$, $f(a_2, \alpha)$, …, $f(a_n, \alpha)$ when α is given, the distribution condition of system data $(A_1, A_2, ..., A_n)$, then the joint probability density function of $(\alpha, A_1, A_2, ..., A_n)$ is $e(\alpha)f(a_1, \alpha)f(a_2, \alpha)..f(a_n, \alpha)$, then the marginal probability density function of $(A_1, A_2, ..., A_n)$ is:

$$f(A_1, A_2, ..., A_n) = \int e(\alpha)f(a_1, \alpha)f(a_2, \alpha)..f(a_n, \alpha)h\alpha \tag{8}$$

Finally, given $A_1, A_2, ..., A_n$, the conditional probability density function of α is as follows [19]:

$$f(\alpha|A_1, A_2, ..., A_n) = \frac{e(\alpha)f(a_1, \alpha)f(a_2, \alpha)..f(a_n, \alpha)}{f(A_1, A_2, ..., A_n)} \tag{9}$$

The above formula is the "a posteriori" probability density function of α. To sum up, it can be concluded that parameter α can be estimated with prior knowledge, such as sample $A_1, A_2, ..., A_n$. It can be found that formula (7) is very similar to Bayesian formula [18]. After knowing the posterior probability distribution $f(\alpha|A_1, A_2, ..., A_n)$, the parameter E can be estimated. Using the above formula, we can get the trust evaluation results of the data in the system. According to the evaluation results, we can provide guarantee for the subsequent information encryption transmission, and choose the appropriate encryption method to process the data with low trust.

2.4 Data Encryption Transmission

According to the above data processing results, the full encryption method is used to encrypt the processed data in this study. The establishment of total homomorphism can be divided into the following steps.

At the beginning of homomorphism, it is necessary to establish a bootstrap [19, 20], which is represented by symbol. Bootstrap should be established according to the

following steps:

$$(wh, oh) \leftarrow K\text{eyGen}_{\lambda}(\delta) \tag{10}$$

$$\Im_i \leftarrow Encrypt_{\lambda}(wh, \wp) \tag{11}$$

$$Decrypt_{\lambda}(oh, \cdot) \rightarrow \wp \tag{12}$$

In the above formula, KeyGen represents the random generation of public key wh and private key oh by random algorithm [21]. On the basis of security parameters, public key defines a clear text space $\Re$ and ciphertext space $\aleph$. $Encrypt_{\lambda}$ means that h is calculated by a random algorithm using valid public key and clear text $\cdot \in \wp$. $Decrypt_{\lambda}$ indicates that the decrypted plaintext $\wp$ is output on the premise of private key wh and ciphertext.

In order to achieve homomorphism, we need to implement an additional process $\cdot \leftarrow Encrypt_{\lambda}(wh, \Re, \wp)$, select $\cdot$ and the generated ciphertext tuple $\wp = (\wp_1, ..., \wp_n)$ from the set of allowed functions, and input them into the circuit [22, 23].

According to the application requirements of Internet of things technology, the possibility of simple attacks in the transmission process should be minimized to ensure the security of fully homomorphic password. Then, when designing the password, we should consider that the selected fully homomorphic password mapping should meet several characteristics.

1. The key space should be large, and its sequence should have good random statistical characteristics
2. Diffusion and confusion
3. Stability

An appropriate encryption process does not guarantee the theoretical and practical security of the sequence cipher with the above three points, but if the above three points are not satisfied, then it is definitely an insecure system. Now, the application of full homomorphic cipher in cryptography is mainly two modes, one is to directly use the data itself to construct the cipher, but its complexity, security and stability need further study. Second, the combination of homomorphic cryptography and the traditional cryptography algorithm with excellent characteristics constructs a new cryptography algorithm, using a new cryptography algorithm to complete encryption. After the encryption links of the above settings are integrated, the proper key is set and the data encryption process is completed.

The content of the design is integrated into the traditional algorithm. So far, the secure data transmission algorithm of remote demonstration system based on Internet of Things is designed.

3 Analysis of Experimental Demonstration

3.1 Experimental Environment Setting

In view of the data security transmission algorithm of the remote demonstration system based on the Internet of things proposed in this study, the experimental link is constructed

to analyze and verify its use effect. The experimental links in this experiment are shown in Table 1.

Table 1. Experimental environment list

Parameter serial number	Parameter	Model
1	Memory	10 GB
2	Operating environment	Intel
3	Database	M4 gmp Crypto++ HElib
4	Programing language	C++
5	Operating system	Windows 10
6	JDK	1.7 and above
7	Other requirements	Interior design function

In this experimental platform, the experimental database of a remote demonstration system is built. In the process of building the experimental database, a variety of basic databases are used. The specific structure is shown in Fig. 3.

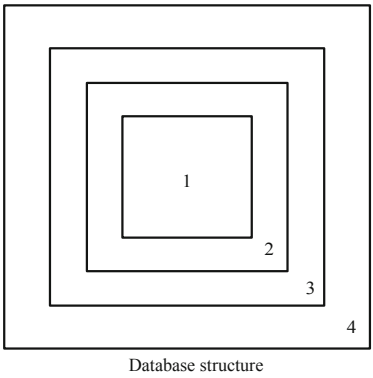

Fig. 3. Structure of experimental database

The relationship between the four related library functions is shown in Fig. 2. One is the GNU version of macro preprocessor; 2. In this experiment, it is used as a mathematical operation library for high precision operation; 3 is a library software that can guarantee multiple floating point calculation; 4 is a C language library which can ensure the correctness of any high-order complex operation. There are 20 groups of data to be transmitted in this data, and the specific data volume and data type composition are as follows (Table 2).

Table 2. Experimental data

Serial number of experimental data group	Data volume/item	Data type
CSSJ-01	896	Data
CSSJ-02	616	Written words
CSSJ-03	882	Image
CSSJ-04	1203	Audio frequency
CSSJ-05	1798	Image
CSSJ-06	541	Written words
CSSJ-07	898	Written words
CSSJ-08	1913	Written words
CSSJ-09	1566	Written words
CSSJ-10	640	Image
CSSJ-11	1695	Image
CSSJ-12	1512	Audio frequency
CSSJ-13	1845	Data
CSSJ-14	1870	Image
CSSJ-15	1132	Audio frequency
CSSJ-16	1772	Audio frequency
CSSJ-17	896	Data
CSSJ-18	616	Data
CSSJ-19	882	Data
CSSJ-20	1203	Written words

The above experimental data is imported into the database, which is used as the data source and carrier in the process of the experiment, and the performance of the proposed Internet of things algorithm is analyzed.

3.2 Setting of Experimental Scheme

In order to make a more detailed analysis of the methods in this study, two kinds of expectations in current use are selected for comparison. At the same time, choose the appropriate experimental indicators to compare the use effect of Internet of things algorithm and traditional algorithm. In this experiment, the experimental comparison index is set as the packet loss rate of data transmission, the number of attacks on data transmission and the amount of data that cannot be read after data processing.

The calculation formula of data transmission packet loss rate is as follows:

$$R = \frac{F_i}{F_{all}} \cdot 100\% \tag{13}$$

In the above formula, F_i represents the data packet successfully sent to the target system; F_{all} is the packet that is trying to be sent to the target system. The above formula is used to calculate the packet loss rate of data transmission.

In this experiment, most of the experimental comparison indicators are statistical indicators. In the process of the experiment, we must ensure the accuracy of data calculation, so as not to affect the authenticity of the experimental results (Table 3).

3.3 Analysis of Experimental Results

Table 3. Packet loss rate of data transmission

Serial number of experimental data group	The packet loss rate of the proposed algorithm/%	Packet loss rate of algorithm in reference [3]/%	Packet loss rate of algorithm in reference [4]/%
CSSJ-01	2.16	5.91	5.08
CSSJ-02	2.63	5.52	5.18
CSSJ-03	2.09	5.66	5.08
CSSJ-04	2.87	5.79	5.33
CSSJ-05	2.61	5.02	5.31
CSSJ-06	2.68	5.91	5.22
CSSJ-07	2.82	5.59	5.56
CSSJ-08	2.02	5.22	5.79
CSSJ-09	2.22	5.03	5.69
CSSJ-10	2.86	5.39	5.19
CSSJ-11	2.48	5.62	5.47
CSSJ-12	2.95	5.21	5.28
CSSJ-13	3.00	5.87	5.15
CSSJ-14	2.35	5.17	5.71
CSSJ-15	2.36	5.43	5.41
CSSJ-16	2.79	5.83	5.29
CSSJ-17	2.11	5.34	5.44
CSSJ-18	2.01	5.13	5.71
CSSJ-19	2.47	5.22	5.73
CSSJ-20	2.16	5.92	5.08

From the above experimental results, it can be seen that the packet loss rate of system data transmission is low after the Internet of things algorithm is used, which indicates that the Internet of things algorithm can effectively control the data loss problem in the process of data transmission, and ensure that the data receiving capacity of the data

receiving node can meet the current data receiving capacity requirements. Compared with the Internet of things algorithm, the packet loss rate of the traditional algorithm is relatively high. In the process of using this algorithm for massive data transmission, there will be a large number of data missing. For the remote demonstration system, a large number of data missing undoubtedly has a direct impact on the use effect of the system. According to the above experimental results, the Internet of things algorithm can effectively guarantee or improve the use effect of the system (Table 4).

Table 4. Attack times of data transmission

Serial number of experimental data group	Attack times of the algorithm proposed in this paper/per time	Attack times of algorithm data transmission in reference [3]/per time	Attack times of algorithm data transmission in reference [4]/per time
CSSJ-01	3	8	7
CSSJ-02	2	7	10
CSSJ-03	3	10	9
CSSJ-04	1	10	8
CSSJ-05	3	5	10
CSSJ-06	1	9	9
CSSJ-07	1	10	10
CSSJ-08	4	6	9
CSSJ-09	4	6	5
CSSJ-10	3	7	7
CSSJ-11	2	5	9
CSSJ-12	3	5	6
CSSJ-13	1	9	7
CSSJ-14	4	5	9
CSSJ-15	4	8	7
CSSJ-16	4	10	6
CSSJ-17	4	8	10
CSSJ-18	4	8	6
CSSJ-19	2	5	6
CSSJ-20	3	8	7

From the above experimental results, it can be seen that the system data transmission is more stable after the application of the IOT algorithm, and in different types of system data, the IOT algorithm can control the transmission security within a fixed interval, so as to avoid the high number of packet transmission attacks affecting the system operation effect. Compared with the Internet of Things algorithm, the traditional algorithm does

not avoid the number of attacks on data, and in the process of data attack, it does not provide adequate protection for data packets, resulting in poor transmission security of data packets. In different types of packets, the traditional algorithm has different effects, which shows that the applicability of this algorithm is low. Based on the above experimental results, it can be concluded that the Internet of Things algorithm is better than the traditional algorithm (Table 5).

Table 5. Abnormal data volume after data transmission

Serial number of experimental data group	The algorithm proposed in this paper abnormal data volume/piece	Number of abnormal data in [3] algorithm/piece	Number of abnormal data in [4] algorithm/piece
CSSJ-01	29	100	118
CSSJ-02	22	109	104
CSSJ-03	28	90	103
CSSJ-04	22	95	109
CSSJ-05	20	110	101
CSSJ-06	28	102	114
CSSJ-07	29	107	109
CSSJ-08	29	101	115
CSSJ-09	25	96	118
CSSJ-10	23	105	120
CSSJ-11	21	102	110
CSSJ-12	29	92	104
CSSJ-13	30	104	106
CSSJ-14	26	97	111
CSSJ-15	29	95	110
CSSJ-16	26	94	114
CSSJ-17	28	90	107
CSSJ-18	27	97	100
CSSJ-19	30	107	110
CSSJ-20	29	100	118

After analyzing the above experimental results, it is found that the abnormal situation of the data transmitted by the IOT algorithm has been alleviated, and the reliability and authenticity of the data transmitted are ensured to some extent. Compared with the Internet of Things algorithm, the traditional algorithm has a relatively poor effect. After completing the system data transmission, it does not reduce the abnormal situation of data transmission, but improves in part of the data. Analysis of the above experimental results can be found that the Internet of Things algorithm based on Internet of Things technology

to complete the data fusion, the data of abnormal problems have inhibition. Based on the above analysis results, it can be concluded that the IOT algorithm is effective.

All the experimental results obtained in this experiment show that the physical network algorithm is better than the traditional algorithm, and it can be used to complete the system data transmission in the future.

4 Conclusions and Prospects

With the development of Internet of things, system data security protection has become an urgent problem to be solved. Data fusion can eliminate redundancy, reduce the amount of data transmission, and then reduce energy consumption. It has become a challenge to secure data transmission while rationalizing the use of data. In this paper, a new data fusion method is proposed, and the effect of the algorithm is analyzed.

In this paper, a secure transmission algorithm of remote demonstration system based on Internet of Things technology is proposed. The bottleneck problem of mass data transmission in physical network is analyzed from three aspects: the defect of SOAP protocol, the defect of application layer and the defect of transport layer, and an improved scheme is put forward to solve each bottleneck problem. Compared with the traditional algorithm, it has some improvements in energy consumption and security, but there are still some deficiencies due to the time and condition constraints, which will be taken as the next step in the research work.

(1) The proposed trust model does not take into account the handling of new nodes.

(2) There is no actual attack test for the proposed data fusion algorithm, only theoretical analysis is carried out, and the next step is to test the algorithm.

(3) This study only considers the integrity of the data, not the robustness of the data. The next step will be to study the algorithm considering the robustness of the data.

Fund Projects. "The National Key Research and Development Program of China" and project number (2016yfb0800700).

References

1. Yang, C.Y., Liu, J.Y.: Data fusion algorithm based on weighted D-S evidence theory in Internet of Things. J. Guilin Univ. Technol. **39**(03), 731–736 (2019)
2. Tu, Y.F., Su, Q.J., Yang, G.: An encryption transmission scheme for industrial control system. J. Electron. Inf. Technol. **42**(02), 348–354 (2020)
3. Shi, L.L., Li, J.Z.: Research and design of secure data transmission mechanism in heterogeneous network. Microelectron. Comput. **36**(11), 84–88+94 (2019)
4. Geng, J.: Simulation of software secret dataloss prevention transmission based on mobile gateway. Comput. Simul. **36**(11), 151–155 (2019)
5. Xu, X.S., Jin, Y., Zeng, Z., et al.: Hierarchical lightweight high-throughput blockchain for industrial Internet data security. Comput. Integr. Manuf. Syst. **25**(12), 3258–3266 (2019)
6. Liu, S., Liu, X.Y., Wang, S., et al.: Fuzzy-aided solution for out-of-view challenge in visual tracking under IoT assisted complex environment. Neural Comput. Appl. **33**(4), 1055–1065 (2021)

7. Fang, W.W., Liu, M.G., Wang, Y.P., et al.: A distributed elastic net regression algorithm for private data analytics in Internet of Things. J. Electron. Inf. Technol. **42**(10), 2403–2411 (2020)
8. Liu, S., Li, Z., Zhang, Y., Cheng, X.: Introduction of key problems in long-distance learning and training. Mobile Netw. Appl. **24**(1), 1–4 (2018). https://doi.org/10.1007/s11036-018-1136-6
9. Gao, P., Li, J., Liu, S.: An introduction to key technology in artificial intelligence and big Data Driven e-Learning and e-Education. Mobile Netw. Appl. **26**, 2123–2126 (2021). https://doi.org/10.1007/s11036-021-01777-7
10. Yu, J.G., Zhang, H., Shu, L., et al.: Data sharing model for Internet of Things based on blockchain. J. Chin. Comput. Syst. **40**(11), 2324–2329 (2019)
11. Zhang, G.H., Yang, Y.H., Zhang, D.W., et al.: Secure routing mechanism based on trust against packet dropping attack in Internet of Things. Comput. Sci. **46**(06), 153–161 (2019)
12. Zhang, T., Zhang, J., Chen, K., et al.: Low-latency data transmission method based on Lora node cooperation. J. Northwest Univ. (Nat. Sci. Ed.) **49**(01), 88–92 (2019)
13. Yuan, M.L., Long, Y., Li, L.: Data transmission algorithms for mobile WSN networks based on piecewise retransmit link awareness mechanism. J. Electron. Measure. Instrum. **33**(12), 50–57 (2019)
14. Harbi, Y., Aliouat, Z., Refoufi, A., et al.: Enhanced authentication and key management scheme for securing data transmission in the Internet of Things. Ad hoc Netw. **94**(Nov.), 101948.1–101948.13 (2019)
15. Xu, J., Tao, F., Liu, Y., et al.: Data transmission method for sensor devices in internet of things based on multivariate analysis. Measurement **157**(25), 107536–107544 (2020)
16. Sujitha, B., Parvathy, V.S., Lydia, E.L., et al.: Optimal deep learning based image compression technique for data transmission on industrial Internet of things applications. Trans. Emerg. Telecommun. Technol. **2020**(6), e3976 (2020)
17. Hasan, M.K., Shahjalal, M., Chowdhury, M.Z., et al.: Real-time healthcare data transmission for remote patient monitoring in patch-based hybrid OCC/BLE networks. Sensors **19**(5), 1208–1215 (2019)
18. Li, X., Zhao, N., Jin, R., et al.: Internet of Things to network smart devices for ecosystem monitoring. Sci. Bull. **64**(17), 1234–1245 (2019)
19. Saracevic, M.H., Adamovic, S.Z., Miskovic, V.A., et al.: Data encryption for Internet of things applications based on Catalan objects and two combinatorial structures. IEEE Trans. Reliab. **14**(9), 1–12 (2020)
20. Duan, R., Guo, L.: Application of blockchain for Internet of things: a bibliometric analysis. Math. Probl. Eng. **21**(6), 1–16 (2021)
21. Gao, Y., Xian, H., Yu, A.: Secure data deduplication for Internet-of-things sensor networks based on threshold dynamic adjustment. Int. J. Distrib. Sens. Netw. **16**(3), 155–162 (2020)
22. Ma, H., Zhang, Z.: A new private information encryption method in internet of things under cloud computing environment. Wirel. Commun. Mob. Comput. **225**(6), 1–9 (2020)
23. Jiang, W., Yang, Z., Zhou, Z., et al.: Lightweight data security protection method for AMI in power Internet of things. Math. Probl. Eng. **15**(5), 1–9 (2020)