A Trusted Transmission Method for Local Multiplexed Data in A Data Center Based on Cloud Computing

Haonan Guo[1], Ziyi Guo[1], Baisheng Liu[2,*]

[1] School of Business Administration, Liaoning Technical University, Huludao 125000, China
[2] School of Software, Liaoning Technical University, Huludao 125000, China

2120011013@stu.Intu.edu.cn

Abstract. With the rapid development of cloud computing technology, the trusted transmission method of local multiplexed data in the data center based on cloud computing has become a hot topic in current research. Traditional multiplexed data transmission methods have problems such as low channel utilization, complex equipment configuration, and poor transmission real-time performance. The trusted transmission method of local multiplexed data in the data center based on cloud computing integrates various types of data such as telemetry, remote control, and experimental data, fully utilizes channel resources, reduces hardware configuration, and improves the flexibility and reliability of transmission. This paper proposes a trusted transmission method of local multiplexed data in the data center based on cloud computing. By establishing a transmission model and adopting an encryption scheme combining symmetric and asymmetric encryption technologies, it optimizes data transmission allocation and ensures data security and integrity. Experimental results show that this method is significantly superior to traditional remote data transmission methods in terms of transmission rate and real-time performance, and is suitable for multiplexed data transmission scenarios. The research in this paper provides new ideas and methods for improving data transmission efficiency and security.

Keywords: Cloud computing; data center; multiplexing; trusted transmission; encryption technology

1 Introduction

With the rapid advancement of technology, local multiplexed data trusted transmission based on cloud computing is continuously improving and has become an inevitable trend [1]. Traditional multiplexed data transmission, while meeting basic needs, has significant limitations: large channel structures requiring extensive cache space, high hardware costs, complex equipment configurations, and low channel utilization, leading to inefficiency and resource waste [2]. Additionally, it struggles with real-time transmission, failing to meet modern demands for speed and flexibility [3].

In contrast, cloud-based local multiplexed data transmission offers superior data processing and broad applicability, making it a research hotspot [4]. By integrating

S. M. Ghadiri et al. (eds.), *Proceedings of the 2025 4th International Conference on Engineering Management and Information Science (EMIS 2025)*, Advances in Computer Science Research 121,
https://doi.org/10.2991/978-94-6463-736-6_17

cloud computing, this method optimizes telemetry, remote control, and experimental data transmission, reducing hardware requirements, complexity, and costs. It also enhances flexibility and scalability, dynamically adjusting weighting coefficients and timeliness to suit diverse transmission scenarios [5-6].

2 Data trusted transmission method

2.1 Establishing a transmission model for local multiplexing data in the middle station

The trusted transmission method of local multiplexed data in the data center based on cloud computing requires first establishing a transmission model for local multiplexed data in the data center [7], and then dividing and transmitting the information at the sender of the information. The network model of multiplexed transmission is shown in Fig. 1.

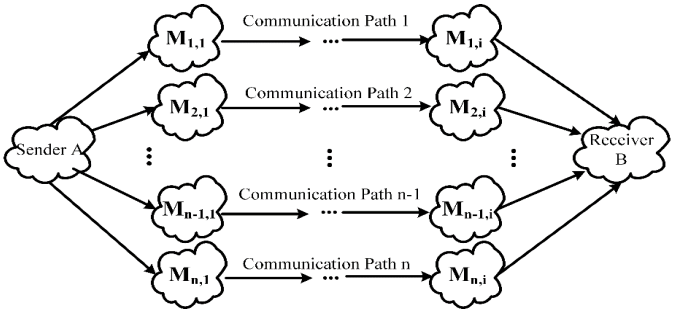

Fig. 1. Multiplexed network model

The routing rules for both parties are as follows:

(1) When there is only one path, data can only be transmitted through that path;

(2) When there are multiple paths, the path should be selected considering factors such as information transmission time and risk of loss.

To address the risk of information loss and ensure accurate delivery, cloud analytics are needed. Each member of the cloud analytics model will provide a different perspective and knowledge. The cloud computing security threat model consists of three parts:

1) Data flow chart: identify nodes that threaten data security, so that program designers can take appropriate security measures for weak links.

2) The entrance and exit of computer programs: the entrance and exit of database programs need to be prevented before sensitive user data enters the database, so it is listed as a key protection point.

3) List of potential threats.

The real threat is in two main areas:

Hackers may tamper with or steal the data sent and received on the client side, so that they can not get valuable information; The staff of the cloud service provider may steal user data from the database. Therefore, effective encryption measures must

be taken after the local area multiplexing data transmission model is established to ensure that the key is not leaked and to protect the security of user information.

2.2 Trusted transmission security encryption based on cloud computing

Trusted transmission security encryption based on cloud computing can prevent information leakage to a certain extent, but it cannot guarantee whether the information will be tampered with. Therefore, this article also uses hash functions to verify the integrity of user data [8].

The implementation of the symmetric cryptographic system requires the use of a symmetric key algorithm [9]. Symmetric key encryption and decryption share a set of keys, which requires the sender and receiver to agree on the key in advance. The security of symmetric encryption is mainly guaranteed by the key, which must be kept confidential. Fig. 2. shows the encryption process of symmetric encryption.

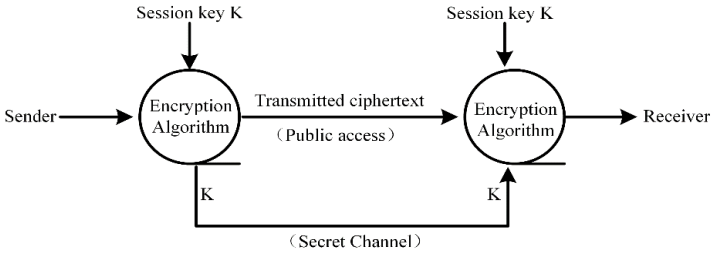

Fig. 2. The process of symmetric encryption

In cloud computing environments, symmetric encryption is often used to protect sensitive data in transit. When users store or transfer data in the cloud, symmetric encryption algorithms can be used to prevent data from being stolen or tampered with during transmission. Symmetric encryption is also crucial in the multiplexed transmission of data in cloud computing. Because of its fast encryption and decryption speed and low resource consumption, it is very suitable for encrypting and decrypting large amounts of data. In multiplexed data transfer scenarios, where data may need to be transferred and accessed multiple times, using symmetric encryption ensures that each transfer and access is adequately protected.

Asymmetric cryptographic system encryption and decryption, asymmetric cryptographic system The sender and the receiver have different keys, and need to use public key and private key. The public key is used to encrypt information, and the private key is used to decrypt information. Fig. 3. shows the encryption process of the public key [10].

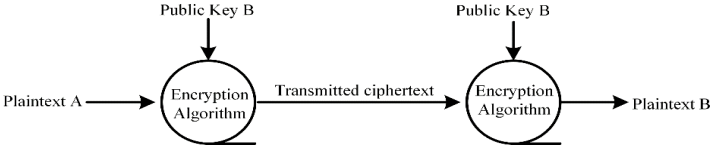

Fig. 3. The process of public key encryption

In a cloud computing environment, asymmetric encryption is often used to ensure the security and integrity of data. For example, during data transmission, the sender can encrypt the data using the receiver's public key to ensure that the data can only be decrypted and accessed by the receiver.

This paper combines symmetric encryption and public key cryptography and adopts digital envelope technology. Digital envelopes have significant advantages. First of all, it combines the advantages of symmetric encryption and asymmetric encryption to ensure the speed and efficiency of data transmission, but also to ensure the security of data. Secondly, the digital envelope can easily manage the key, avoiding the risk of the key being stolen in the process of transmission. Finally, the digital envelope can also be used to realize the separation of data encryption and decryption operations, improving the flexibility and scalability of data transmission. Cloud computing users do not need to purchase high-performance hardware. Cloud computing integrates multiple technologies to provide cross-device data and application sharing services. Users can access the same record on different devices, which greatly improves the convenience of use. Cloud computing breaks through the limitations of individuals and single devices. Its programming model is simple and easy to learn, which simplifies programming in the cloud environment. Cloud computing has massive data distributed storage and management technology, runs on low-cost hardware, and provides fault tolerance. Based on the distributed transmission method, cloud computing provides users with more comprehensive services in the macro sense, has strong compatibility, low requirements on device performance, and is suitable for ordinary hardware. Many IT companies have adopted cloud computing as a data storage technology.

There are also many problems that need to be overcome in the use of cloud computing, such as how to ensure its security. To ensure the security of cloud computing, we should pay attention to the following two aspects [11]:

1) Credibility: Cloud computing must gain the trust of users. Only in this way can users dare to put their data in the cloud environment. Therefore, the stability, reliability and confidentiality of cloud computing are crucial. Only in this way can we win the favor of users. Users dare to store their data in the cloud service end.

2) Privacy: At present, individual users are the main objects of cloud computing services. In this process, privacy is very important. To ensure the privacy protection of users, many security protection technologies will be used.

We must ensure the security of user data transmission and storage to guarantee file confidentiality and privacy. Effective methods are needed to protect data from tampering or theft when uploaded from the user end. Encrypting disguises messages to hide content, while decrypting restores encoded data to its original form, reversing the encryption process.

Encryption technology includes two major elements: algorithm and key [12]. The encryption process depends on the encryption algorithm and key. Only one of them needs to be kept secret to ensure the security of the ciphertext. The key must be strictly confidential and the number must be large to resist cracking; at the same time, the encryption transformation must be complex enough to force attackers to use exhaustive methods to crack. However, these algorithms are not absolutely secure in theory

and are usually used in non-critical or confusing scenarios. A truly secure encryption algorithm must be able to resist attacks such as differential analysis. In encryption operations, specific bits (such as the 8th and 16th bits) are used as check bits, and the key is securely exchanged through the "public key transmission method". This method is opposite to the "symmetric encryption algorithm" and is called the "asymmetric encryption algorithm". The working principle of the key generation and information encryption module is shown in Fig. 4.

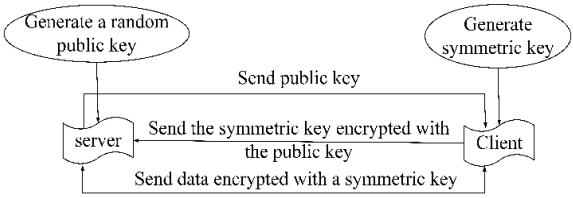

Fig. 4. Working principle diagram of key generation and information encryption module

The most representative asymmetric encryption algorithm is the RSA algorithm. The RSA public key encryption algorithm is the most effective public key encryption algorithm today, and it can effectively resist all known password attack methods.

The security of RSA relies on large number factorization, where both the public and private keys are generated from two large prime numbers (more than 100 decimal numbers). Speed has always been a weakness of RSA, which is usually only used to encrypt small amounts of data.

2.3 Optimize data transfer distribution

The cloud computing transmission method is a large and comprehensive transmission method that cannot be completed by a single person [13-14]. Therefore, the cloud computing transmission method designed and implemented in this paper only has some basic characteristics of cloud computing. The main server node does not directly store user data and is only responsible for the management of sub-nodes and users. The client of cloud computing can be a variety of devices, such as desktop computers, notebooks, and mobile phones. At this time, the important data to be transmitted must be encrypted. Two transmission method data files will be saved in the main server node: root.dat and node.dato root.dat. Fig. 5. shows the cloud computing resource allocation sequence diagram.

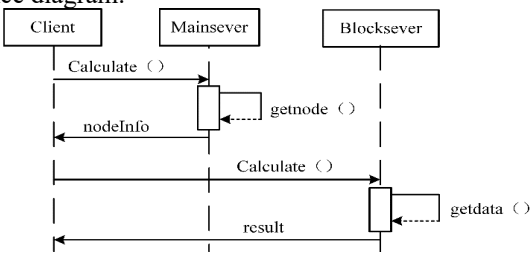

Fig. 5. Cloud computing resource allocation sequence diagram

In Fig. 5., the client starts the cloud computing service only after communicating with the main server and the main server intelligently distributes the node data to the client. The client will establish a connection with the computing node based on the node data and pass the corresponding results to the client.

Multiple subnodes form a block server subnode for cloud computing data blocks. The client sends data to each node, which processes and returns results for aggregation. Calculations occur on the node storing the data, following client instructions to enhance work rate. This method significantly boosts efficiency for large-scale data processing.

3 Experiment

3.1 Experimental methods

Five computers are prepared for the traditional remote data transmission method and the local multiplexing data trusted transmission method based on cloud computing. All specifications of the computer are the same, specifically, the processor specifications: 11th Gen Intel(R) Core (TM) i5-1135G7 @ 2.40GHz 2.42GHz; The basic frequency of the processor is 2.40GHz, in addition, each computer is configured with 16GB of memory, the network speed is the same, and it is a private network to ensure the efficiency and stability of data processing during experiments or research. The traditional remote data transmission method is installed with Windows environment, and the local multiplexing data trusted transmission method based on cloud computing is installed with Unix simulation environment.

This paper conducts experiments on the traditional remote data transmission method and the local multiplexing data trusted transmission method based on cloud computing. The experimental methods are as follows:

(1) Five construction sites in the same city are selected, and the monitoring images of these five construction sites are uploaded to the computer room of the monitoring center at the same time;

(2) The traditional remote data transmission method and the local multiplexing data trusted transmission method based on cloud computing upload the same monitoring image data five times at different time intervals in a week. Each time when uploading the image, the network traffic of the two transmission methods is basically the same;

(3) The upload time of the uploaded image data is counted.

3.2 Experimental results and analysis

After conducting the experiment according to the above experimental method, the experimental data were sorted and summarized, as shown in Table 1. Based on the simultaneous uploading of experimental data from 5 experimental sites, the average upload rate of the traditional remote data transmission method, the construction site remote monitoring transmission sub-transmission method, is lower than the upload rate of the cloud computing-based data center local multiplexing data trusted trans-

mission method, the construction site remote monitoring transmission sub-transmission method.

Table 1. Experimental summary data

Upload image data			Traditional method		The method proposed in this paper	
Number of uploads (/times)	Quantity (/pcs)	Quantity (/M)	Upload time (/s)	Upload rate (k/s)	Upload time (/s)	Upload rate (k/s)
First time	6	508	6053	85.9	5642	92.2
Second time	6	600	7877	78.0	6468	95.0
Third time	7	466	5798	82.3	5093	93.7
Fourth time	8	684	8799	79.6	7119	98.4
Fifth time	7	680	10331	67.4	7292	95.5
Average	-	-	7771.6	78.64	6322.8	94.96

Although the hardware and network speed of the experiment are the same, and the experiment time is the same, there may be small errors due to the distance between the experimental sites. Experimental results show that the average speed of the cloud computing-based local multiplexed trusted transmission method in data center is higher than that of the traditional remote data transmission method.

In the test experiments in this paper, we compare the effects of two transport strategies: the first is the Priority Policy-Based Transport Method (PBT); The second is the traditional remote data transfer method that employs a progressive image transfer strategy. By comparing the response time of the two, the efficiency of the two transmission strategies was evaluated.

In addition, this paper evaluated the difference significance between our method and the traditional method from the aspect of mathematical statistics: Wilcoxon test. The obtained data p=0.0079, p value is less than the significance level (usually set at 0.05), then the null hypothesis can be rejected and it is considered that there is a significant difference in the median of the two samples. Therefore, we can conclude that the transmission rate of our method is higher than the upload rate of traditional remote data transmission methods.

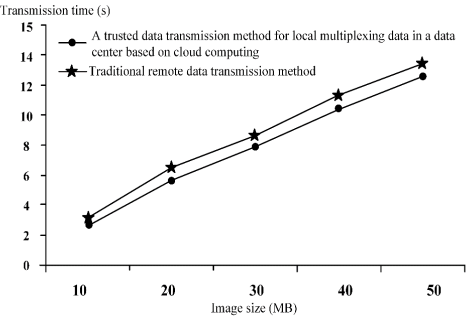

Fig. 6. Time required to transfer a complete image

In Fig. 6., when transmitting the same surveillance image, the transmission time of the local multiplexing data trusted transmission method based on cloud computing data center is shorter than that of the traditional remote data transmission method. This is because the traditional remote data transmission method is a real-time processing transmission method that requires a time-consuming processing process. The local multiplexing data trusted transmission method based on cloud computing data center in this paper processes the complex processing process offline. When a request is received, the processed image data can be directly retrieved and transmitted, and the real-time transmission is stronger. Fig. 7. shows the time required to obtain a partial image of the data.

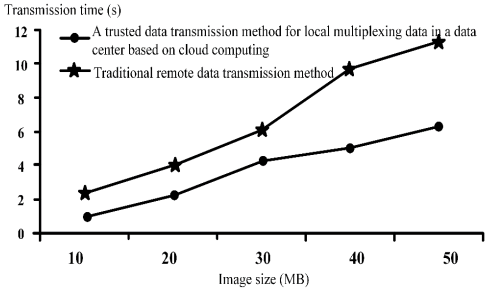

Fig. 7. Time required to obtain the image of the data part

Comparing Fig. 7 and Fig. 6, it can be seen that the time required to obtain a complete image is much longer than that required to obtain a partial image. This is because the cloud computing-based transmission method can transmit relevant data in a timely manner. Fig. 6 shows that the cloud computing-based data center local multiplexing transmission method proposed in this paper takes less time than the traditional remote transmission method when transmitting partial images. Although the traditional method supports priority transmission, the algorithm is complex and the processing time is long, which indirectly increases the transmission time. Therefore, the cloud computing-based transmission method effectively improves the rate of traditional remote transmission and enhances the accuracy and expansion capability of multiplexed data.

4 Conclusion

The experiment designed in this paper compares the data transmission rates of cloud computation-based data center local multiplexing trusted data transmission method and traditional remote data transmission method. The experimental results show that the average data transmission rate of cloud computation-based data center local multiplexing trusted data transmission method is much higher than that of traditional remote data transmission method. Therefore, the method proposed in this paper is more suitable for transmitting multiplexed data.

However, although the method proposed in this paper shows advantages in experiments, it still has limitations. First of all, the security of the cloud computing environment deserves attention. Despite the discussion of encryption techniques and hash

functions to ensure the integrity and confidentiality of data, cloud computing platforms can still face security threats such as hacking attacks, data breaches, and more. Therefore, security protection measures should be strengthened in practical applications to improve the overall security of data transmission.

Future research directions include optimizing the cloud-based data center station local multiplexing transmission method. On the one hand, it can strengthen the research on the security of cloud computing environment and develop more advanced data encryption and privacy protection technology; On the other hand, the optimization strategies of the transmission model can be deeply studied, such as improving the routing algorithm and data transmission allocation, to further improve the transmission efficiency and stability.

References

1. Yang, Changsong, et al. "Secure data transfer and deletion from counting bloom filter in cloud computing." Chinese Journal of Electronics 29.2 (2020): 273-280.
2. Zhang, Peiying, et al. "A reliable data-transmission mechanism using blockchain in edge computing scenarios." IEEE Internet of Things Journal 9.16 (2020): 14228-14236.
3. Ramirez, Carlos Erazo, et al. "HydroRTC: A web-based data transfer and communication library for collaborative data processing and sharing in the hydrological domain." Environmental Modelling & Software 178 (2024): 106068.
4. Ke, Malong, et al. "Massive access in cell-free massive MIMO-based Internet of Things: Cloud computing and edge computing paradigms." IEEE Journal on Selected Areas in Communications 39.3 (2020): 756-772.
5. Li, Dali. "Virtualization and energy management optimization of high speed computer network data centers based on optical switching and network technology." Thermal Science and Engineering Progress 55 (2024): 102918.
6. Yaothanee, Jumpol, and Kasidit Chanchio. "A checkpointing mechanism for virtual clusters using memory-bound time-multiplexed data transfers." International Journal of Electrical and Computer Engineering (IJECE) 14.1 (2024): 1147-1165.
7. Yaothanee, Jumpol, and Kasidit Chanchio. "A checkpointing mechanism for virtual clusters using memory-bound time-multiplexed data transfers." International Journal of Electrical and Computer Engineering (IJECE) 14.1 (2024): 1147-1165.
8. Ganeeb, Koushik Kumar, et al. "Advanced encryption techniques for securing data transfer in cloud computing: A comparative analysis of classical and quantum-resistant methods." KK Ganeeb, V. Jayaram, MS Krishnappa, P. Gupta, A. Nagpal, AR Banarse, and SG Aarella," Advanced Encryption Techniques for Securing Data Transfer in Cloud Computing: A Comparative Analysis of Classical and Quantum-Resistant Methods," International Journal of Computer Applications 186.48 (2024): 1-9.
9. Ganeeb, Koushik Kumar, et al. "Advanced encryption techniques for securing data transfer in cloud computing: A comparative analysis of classical and quantum-resistant methods." KK Ganeeb, V. Jayaram, MS Krishnappa, P. Gupta, A. Nagpal, AR Banarse, and SG Aarella," Advanced Encryption Techniques for Securing Data Transfer in Cloud Computing: A Comparative Analysis of Classical and Quantum-Resistant Methods," International Journal of Computer Applications 186.48 (2024): 1-9.

10. Ming, Yang, et al. "Generic Construction: Cryptographic Reverse Firewalls for Public Key Encryption with Keyword Search in Cloud Storage." IEEE Transactions on Cloud Computing (2024).
11. Yanamala, Anil Kumar Yadav. "Emerging challenges in cloud computing security: A comprehensive review." International Journal of Advanced Engineering Technologies and Innovations 1.4 (2024): 448-479.
12. Olaiya, Omolara Patricia, et al. "Encryption techniques for financial data security in fintech applications." International Journal of Science and Research Archive 12.1 (2024): 2942-9.
13. Mark, John, and Revathi Bommu. "Tackling Environmental Concerns: Mitigating the Carbon Footprint of Data Transmission in Cloud Computing." Unique Endeavor in Business & Social Sciences 3.1 (2024): 99-112.
14. Zhong, Z. O. N. G. "Research on the secure Transmission Method of Cloud Computing Data." 2021 16th International Conference on Computer Science & Education (ICCSE). IEEE, 2021.