Research on Big data Security privacy Protection based on cloud Computing

Tongtong Xu 1, *, Lei Shi 2
1 School of Management, Tianjin University of Technology, Tianjin, China
2 School of Management, Tianjin University, Tianjin, China

*Corresponding author e-mail: xutongtong@tjut.edu.cn

Abstract. Cloud computing is a new way of computing and storage. Users do not need to master professional skills, but can enjoy convenient network services as long as they pay according to their own needs. When we use cloud services, we need to upload data to cloud servers. As the cloud is an open environment, it is easy for attackers to use cloud computing to conduct excessive computational analysis on big data, which is bound to infringe on others' privacy. In this process, we inevitably face the challenge of data security. How to ensure data privacy security in the cloud environment has become an urgent problem to be solved. This paper studies the big data security privacy protection based on cloud computing platform. This paper starts from two aspects: implicit security mechanism and display security mechanism (encryption mechanism), so as to protect the security privacy of cloud big data platform in data storage and data computing processing.

1. Cloud Data security privacy protection overview

1.1. Cloud computing security and privacy issues

Cloud computing is a new computing method based on the Internet, which is different from the traditional computing mode. In this way, the software and hardware resources and information shared on the cloud platform can be provided to many computers and other network devices on demand. There are three service modes of cloud computing, namely SaaS, PaaS and IaaS.

The security issues of cloud computing mainly include whether the data stored on the cloud platform is secure; Whether users' operations on the cloud platform can be monitored, replayed, or tampered with; Whether the cloud platform itself is reliable, whether the services provided by the cloud platform are correct, whether the cloud platform, and whether the cloud service provider charges arbitrarily. These security problems mainly come from two aspects: on the one hand, cloud service providers are dishonest and unreliable; on the other hand, cloud platforms may be attacked or invaded from outside.
1.2. Big data security and privacy issues
Thanks to the technology of big data, users can buy more suitable products at a lower price, but at the same time, a large amount of data about individuals’ shopping habits, financial situation and even health status will be collected by the platform. A large number of server data leaks in recent years show that if the security and privacy issues of big data are not properly solved, it is likely to bring incalculable losses to individuals, enterprises and even the country. According to the different privacy contents to be protected, privacy protection can be further divided into connection relation anonymous protection, identifier anonymous protection and location information privacy protection. On the whole, the current big data mainly has four security issues: infrastructure security, storage security, network security and privacy security.

2. Privacy protection system for big data security under cloud computing
2.1. System function design
The main functional modules of the system include user login module, file upload module, file download module, computing module, file retrieval module and data management module, etc. The system structure is shown in the figure below:
2.2. Detailed design and implementation of privacy protection system

2.2.1. Design and implementation of user login function. Before entering the system, users need to choose to log in, register or log out. Flow chart of the user login validation choose login, users need to enter your user ID and password to log in, if verification is successful, directly into the system, if validation fails need user registration account, according to the symmetric Key generated password Key user registration, at the same time to cloud the server application, cloud service generates an asymmetric Key pair, Send the public Key to the client. The client encrypts the Key with the public Key and sends ciphertext CKey to the cloud server. The cloud server writes Key Ckey, private Key private Key, user ID, and password Hash value PWD to the user information table in the system database. If true is returned, registration is successful; otherwise, registration fails.

2.2.2. Privacy data upload module function design and implementation. User input to the path of the uploaded file, choose whether to encrypt, if encryption is not directly stored in the cloud, if encryption system will also have a file hash value of data privacy, the privacy data and the hash value split, system will be based on user input password for symmetric Key Key, to encrypt the data after the split. Ciphertext transmission brought cloud services, cloud server call private Key private Key Key decryption Key get symmetric Key cipher Key, using the Key decrypted plaintext message, to isolate the hash value is calculated after private data Z’, and decrypt the hash value Z contrast, its purpose is to validate data integrity, test cipher text in the process of transmission have been illegally tampered with. If Z’=Z, the ciphertext is stored in the cloud storage module and the storage address is returned. The cloud server writes the storage address, file name, and file secret level into the database and returns true to the client, indicating that the upload is successful. If Z’≠Z, the data is rejected and false is returned to the client, indicating that the upload fails.

2.2.3. Function design and implementation of private data download module. After the user enters the file name, the cloud server obtains the file information storage path from the database according to the file name and obtains the file from the corresponding location. Then the cloud server sends the file and the file secret information to the client. The client checks the security level of the file. If security is 0,
the file is output directly. If security is 1, the client uses the symmetric Key to decrypt the ciphertext, extract the private data, and calculate the summary value Z. If Z \( \neq Z \), output private data, otherwise download fails.

2.2.4. Design and implementation of computing functions. This feature uses cloud computing to perform a simple addition operation. The client input a set of data, calculates the summary Z, assembles the data, encrypts it and transmits it to the cloud server. After decryption, the cloud server verifies data integrity and computes sum after the verification passes. Calculate the summary value of sum Z', combine it with the calculation result, encrypt it and transmit it to the client, the client verifies the data integrity, and output the sum result after passing it.

2.2.5. Database design. The system database uses My SQL database, which describes the field names and data types of entities. The main description content is shown in the following table.

| Table 1. Table1. User information |  |
|-----------------------------------|--|
| The field name | The data type |
| Id | long |
| User Id | varchar |
| Pwd Hash | varchar |
| CKey | medium text |
| Private Key | varchar |

| Table 2. Fileinformation |  |
|--------------------------|--|
| The field name | The data type |
| Id | long |
| Name | varchar |
| Size | long |
| Place | varchar |
| Security | varchar |

2.3. Security analysis
Analysis is made from the perspective of encryption technology and cloud computing platform.

2.3.1. Encryption technology Angle. The further optimized AES algorithm uses double symmetric key to improve the security of symmetric key. SM2 asymmetric encryption algorithm is used to encrypt symmetric keys, which can ensure the security of key distribution. Each transfer checks the integrity of the data to see if it has been tampered with. The cloud server saves private data in the form of ciphertext in the cloud, which ensures the storage security of private data to a certain extent.

2.3.2. Cloud computing platform perspective. Ali Cloud ECS provides DDOS protection capabilities, cloud monitoring capabilities and a variety of real-time alarm capabilities. Therefore, the cloud platform chosen is relatively safe.

To sum up, the privacy protection system is designed based on the hybrid encryption scheme of improved AES algorithm and SM2 algorithm, which can ensure the security of private data transmission in the cloud environment. The experimental results show that the system can not only improve the decryption difficulty of symmetric key, but also ensure the security of symmetric key distribution, and the decryption speed of the system has been rapidly improved. Compared with other hybrid encryption schemes, the scheme in this paper has been improved in security and encryption and decryption speed, and has better practicability.
3. Summary and Prospect
With the development of recent years, cloud computing has made great progress and innovation, the development of cloud computing has brought us a lot of convenience, but also brought us a lot of security problems. For the security and privacy protection of big data under cloud computing, encryption technology can be used to ensure the accuracy and confidentiality of cloud privacy data. The big data security problems of cloud computing can effectively improve the development of cloud computing platform and make important contributions to the economic and social development of our country through the corresponding protection of users through the due information.

References
[1] Li Xi. Analysis of Data security and Privacy Protection in Cloud Computing Environment [J]. Network Security Technology and Application, 2021(08): 70-72.
[2] Huang Liang, Chen Li, Ma Ming. Big data security and privacy protection based on cloud Computing [J]. Electronic Technology and Software Engineering, 2020(24): 249-250.
[3] Guo Fei. Analysis of data security and privacy protection in cloud Computing Environment [J]. Digital Communication World, 2019(06): 125+182.
[4] Pang Haoyuan. Data security and privacy protection in cloud computing [J]. Science and Technology Innovation, 2019(03): 103-104.
[5] Wang Xiaogang. Research on data security and privacy protection in hybrid cloud computing [J]. Information security and technology, 2015, 6(07): 38-39+53.
[6] Liu Meng, Xie Zanfu. Discussion on privacy protection and data security model of cloud computing [J]. Journal of Guangdong Polytechnic Normal University, 2012, 33(09): 32-34.