Data Security Analysis in Cloud Computing Environment

Zhang Yilin, Gui Xiaolin, Gong Jun, You Zhen, Cheng Si

Jiangxi Normal University, Nanchang, Jiangxi, China

Keywords: Cloud Computing, Data Security, Big Data

Abstract: with the breakthrough of computer software and hardware technology and the popularization of big data in China's commercial application, more and more small and medium-sized enterprises choose cloud technology as the way to build their own data center, but with it comes an increasingly urgent data security problem. In the cloud computing environment, there are many data security problems, not only data leakage security accidents, but also a few According to the safety accident of data loss. Therefore, based on the specific problems of data security in big data and cloud computing, combined with the application of data security technology, this paper makes a comprehensive analysis of data security in cloud computing environment.

1. Introduction

With the rapid development of information technology, the application of cloud computing technology is more and more popular, and the data security problem is more and more prominent, which directly threatens the business data and personal privacy data of enterprises. Especially with the advent of the era of big data cloud computing, data has become a kind of production material that is worth exploring, but it also brings more data security problems to people. Once the massive data collected by enterprises is leaked, the loss may be incalculable. In the face of the increasingly complex cloud computing environment, to better solve the data security problem, this paper starts from the relationship between big data and cloud computing, combined with specific issues for in-depth discussion.

2. The Relationship and Advantages of Big Data and Cloud Computing

2.1 The Relationship between Big Data and Cloud Computing

Since the new century, big data technology and cloud computing technology have been popularized with the improvement of computer hardware. Among them, big data refers to the collection of data that can be acquired, managed and analyzed. The range of this collection is far beyond the processing capacity of traditional database software tools. Its data flow is relatively faster, the data volume is relatively larger, and the data types are relatively more diverse. The technical classification of big data is shown in Figure 1. The main function of big data technology is to help enterprises or individuals to collect and process data more efficiently. By processing big data, enterprises can find the association between different data from massive data, thus providing basis for decision-making. Cloud computing is the premise of the implementation of big data technology. Cloud computing refers to distributed computing technology, which enables the implementation of algorithms to be completed by different computers. In practice, big data and cloud computing are also closely linked. Big data technology needs a distributed architecture to run related algorithms. It takes distributed algorithm as its main feature, cloud computing, distributed database and cloud storage technology as its support, and finally realizes data mining of massive data. The real-time analysis of big data mostly uses the architecture similar to MapReduce to allocate work to multiple computers. Only with the support of this special algorithm architecture, the processing of big data will become efficient.

  DOI: 10.25236/ISMHI.2019.082

Fig.1 Big Data Technology Classification

Big data technology classification	Big data technology and tools
Infrastructure support	Cloud computing platform, cloud storage, virtualization technology, network technology, resource monitoring technology
data acquisition	Data bus ETL tool
Data storage	Distributed file system, relational database NoSQL technology, integration of relational database and non relational database, memory database
Data calculation	Data query, statistics and analysis, data prediction and mining
Data presentation and interaction	Graphics and reports, visualization tools, augmented reality technology

2.2 Advantages of Big Data and Cloud Computing

The application advantage of cloud computing technology mainly lies in the dynamic adjustment of data processing and operation. Because of cloud computing, the data capacity of the server can be expanded by adding idle processors, so that the processing capacity of the server can be planned and expanded according to the needs of users, so that the computing resources can be fully utilized. Cloud computing also provides a variety of possibilities in the choice of Internet access methods. On the one hand, enterprises can limit the impact of possible malicious behavior of users on the server by limiting the bandwidth; on the other hand, different rights accounts provided by enterprises also limit the behavior of users when using cloud computing.

Overall, the advantages of cloud computing lie in optimizing industrial layout and promoting professional division of labor. In terms of optimizing the industrial layout, cloud computing reduces the space for small companies to operate data centers, and makes cloud computing industry resources gather to Alibaba, Tencent, Baidu and other large Internet companies, which not only makes it industry more centralized, but also makes other enterprises with demand for data centers more dependent on these Internet companies. In terms of optimizing the industrial layout, cloud computing reduces the cost of building and maintaining data centers, enables enterprises to spend more on their main businesses, reduces the cost of enterprise operation and management, and improves the overall efficiency of enterprises.

In addition, the advantages of big data cloud computing are reflected in the flexibility of use and the convenience of management. Because cloud computing technology is a kind of virtual technology, it can link all data resources, and then provide convenience for users to find corresponding data resources on the basis of cloud operating system. In this process, the time to query resources is related to the rated computing power of the cloud computing server. Because the hardware management of this virtual technology application is in the charge of the specific cloud computing service provider, it is also easier for the enterprise to maintain and manage.

3. The Importance of Data Security and Data Security in Big Data Cloud Computing Environment

3.1 The Importance of Data Security in Big Data Cloud Computing Environment

With the popularization of mobile Internet technology, the behavior of collecting data from users is becoming more and more common, but there is no perfect way to use and protect these data. Although enterprises have collected massive data about users through big data and cloud computing, they have not established a perfect protection mechanism to protect these data, resulting in more and more user data being exposed in the network for various reasons and even used for transactions, so the network security problem is more and more prominent. Although cloud computing provides convenience for enterprises in reducing the cost of data center construction, it also makes user data more centralized, and the loss caused by data leakage security accident in cloud computing center is greater. Therefore, the prevention and solution of data security problems become more important.

3.2 Data Security in Big Data Cloud Computing Environment

The security problems of big data cloud computing are reflected in many aspects. The main data security problems are as follows:

The first is the security of data isolation. This security problem mainly occurs in the data sharing process of cloud computing system. At present, because cloud computing users are mainly collective users, and enterprise accounts for a large proportion, data isolation technology of cloud computing service providers is tested for data isolation of different enterprises. Because of the demand of resource sharing in the operation of enterprises, the data mobility in the enterprise cloud computing server is strong. If we want to ensure the data sharing characteristics, it is difficult to protect these data with strict encryption. This makes it easy for hackers to obtain data information of enterprises by destroying the sharing mechanism through external computers without isolation measures. Therefore, how to improve the data isolation mechanism and establish the firewall system of cloud computing are the first issues that cloud computing service providers need to consider.

Secondly, data access security. Illegal access is an important manifestation of data access security issues. Illegal access may be implemented by external users or internal technicians of cloud computing service providers. Such access is often implemented by obtaining permission accounts, so it is more difficult to find and prevent. In particular, the hardware part of cloud computing server is almost completely maintained by cloud computing service providers. It is easier for technicians to obtain the data stored in the data center by technical means, which also makes some technicians profit by stealing and reselling enterprise data driven by interests. Therefore, it is very important to design data access security operation specifications to prevent data access security problems.

Finally, data security problems caused by data corruption. Because the data collection, storage and processing in cloud computing services are often procedural, in order to ensure the security of data, many data are often destroyed after reading and using to ensure that it will not be obtained by third parties. But part of the data is often stored in the memory of cloud computing, which is not cleaned up immediately. These incomplete destruction sometimes affect the security of the data system. If the data is not completely destroyed, the hackers may master the storage law of cloud computing algorithm after data leakage, thus increasing the possibility of data leakage and increasing the risk of enterprise data leakage. In addition, the data destruction of big data often takes a long time, which also makes the risk of data leakage further increased. In addition, the security vulnerabilities of cloud computing system may also lead to data leakage. Hackers often obtain the data stored in cloud computing server through these vulnerabilities.

4. Data Security Measures in Big Data Cloud Computing Environment

In order to ensure the data security in the big data cloud computing environment, we can strengthen the protection of data security from the following aspects by combining technical means:

First of all, we need to strengthen the isolation of cloud computing system from data. Specific isolation means include data isolation and protection, server isolation, storage isolation and network isolation. Data isolation and protection is usually the design of storage access rights, which protects data by restricting the access rights of different users and different files. Server isolation ensures the reliability of application by means of dual backup. Storage isolation uses physical isolation or Lun access control to protect data, while network isolation uses VLAN to ensure network isolation. Although there are many methods for data isolation, it is still difficult to avoid data leakage or damage due to the operation of internal personnel or authorized accounts.

Therefore, the second point is to strengthen the identity authentication and authority management of the internal personnel of cloud computing service providers, strictly limit the operation authority of the employees at all levels of cloud computing service providers, and introduce security organs to help cloud computing service providers carry out security supervision and management, so as to enhance mutual trust between employees and enterprises. In addition, the identity authentication system also requires the sensitive operation of relevant personnel to automatically report to the top-level supervisor, so that the enterprise can detect and respond to the illegal access accident in

time.

Third, the application of data backup technology. In the cloud computing environment, when the data security accident occurs, the system may take the automatic deletion of sensitive data as the most direct means of protection, and the recovery of these data after the event is likely to be realized through data backup technology. And with the continuous improvement of technical level, the possibility of data destruction will be more and more big. The possibility of data damage and its possible impact after damage are more and more, so it is necessary to pay attention to the application of data backup, design the corresponding backup cycle and the backup system with strict defense, so that the backup data can be more strictly protected.

Fourth, strengthen data access control. In the cloud computing environment, strengthening access control is also an important way to protect data security. Because cloud computing needs to deal with a large number of data, the access behavior of ordinary users to the server is quite different from that of malicious users. For example, hackers may make the server vulnerable through frequent access to the server, which can be identified and suppressed by access control technology. There are many kinds of access control technologies, including role access control, autonomous access control and forced access control. From the perspective of autonomous access control, each object is the owner with control right. The structure of permission is relatively simple and the scope of application is wide, but the possibility of cracking the access right is also large. Mandatory access control implements access control by classifying tags. The role access control technology realizes the access control by combining with the layered scheme.

Finally, we pay attention to the application of data encryption technology. In order to ensure the security of data, data encryption technology based on various algorithms becomes very important, and makes cryptography become a specialized independent discipline in modern times. In data processing, data will be packaged and sent to cloud computing data center after being encrypted. In order to distinguish different user areas, metadata encryption must be done well. These information are encrypted by the key produced according to the algorithm, and then decrypted by the special decryption key. When there is no decryption key for illegal access, these data are difficult to be read and applied directly, so that the data security is protected.

5. Conclusion

To sum up, in the era of big data cloud computing, strengthening data security management becomes more and more important. In the face of many data security threats, we should pay full attention to the application of data security technology, and improve the data security performance of cloud computing service providers and devices from the aspects of software and hardware. Through the above discussion of data security and corresponding safeguard measures, I hope to play a positive role in solving the actual data security problems to a certain extent.

References

[1] Yang Li.(2018). Information security and protection in cloud computing environment [J]. Information recording materials, no.11,pp.71-72

[2] Xu Ziming.(2018). Data security analysis in big data cloud computing environment [J]. Electronic technology and software engineering, no.20,pp.193

[3] Bai Xiao.(2018).Data security in big data cloud computing environment [J]. Computer programming skills and maintenance, no.11,pp.164-166

[4] Huang Xin.(2019).Data security research in big data cloud computing environment [J]. Information communication, no.01,pp.194-195