Research on Big Data Security in the Cloud Computing Environment

Lijun Mao

Xi'an Peihua University, Xi'an, Shaanxi, 710125, China

Keywords: Cloud computing; big data; security.

Abstract: On the basis of cloud computing environment, the big data files stored by computer users may suffer malicious or unintentional leaks or even damage from some unreliable cloud service providers. For those cloud service users who are lack of local data backup, it is necessary to further improve the security storage method of big data and effectively eliminate the hidden dangers of big data by implementing the audit of periodicity and integrity of big data files. In this paper, it outlines the basic meaning of cloud computing, analyzes the outstanding advantages of cloud computing, analyzes the security of big date in the cloud computing environment, and puts forward some ideas to ensure the security of big data in the cloud computing environment.

1. Introduction

Big Data in the cloud computing environment is built on the new network technology under the premise of network information technology. Using the virtualized network platform, users can store and process data, and can use the network to transmit data to users again. As a new form of data processing, big data security technology in cloud computing has higher efficiency and larger capacity than previous data processing form, which has gradually become the mainstream data processing form. However, there are some security risks in big data under cloud computing. Facing with the huge demand for big data in modern society, how to further improve the security problem under the big data in cloud computing environment has become an important issue for big data technology practitioners.

2. Basic Meaning of Cloud Computing

The so-called cloud computing refers to one of the calculation forms to process data and transfer computer resources by using network, and to reflect the trend of dynamic development, which can be easily expanded on the premise of Internet computing, distributed processing and parallel processing. Compared with the traditional computer computing form, cloud computing can virtualize date with low cost and strong security and reliability, and is easy to be expanded, stored and highly computed to achieve the goal of resource sharing. Modern people are increasingly recognizing cloud computing. However, as cloud computing becomes more widely used, it will bring more risks to enterprises and individuals while bringing convenience to modern people, thus posing a great challenge to the development of modern enterprises.

3. Outstanding Advantages of Cloud Computing

First, the cost of input is quite low. Traditionally, data center must have a relatively high cost, so a large number of SMEs cannot create their own data management center due to they cannot pay higher fees. However, cloud computing can provide a very good development condition for the development of SMEs. These enterprises can rent services they needed by fully using of cloud computing services, which promotes the overall cost reductions, and is very conducive to the sustainable development of the enterprise for it does not require very complicated management. Second, the amount of resources covered is very large. Cloud computing resources belong to a very large resource pool, which is mainly constructed by many computer resources and can share resources. Network is mainly used for

  DOI: 10.25236/systca.18.085

access, so users can use the hardware and software in the cloud computing resource pool. Such ultra-large-scale resources can greatly enhance the data access function of users, and the data storage and computing capabilities can also be improved. Third, the dynamic of the date is achieved. The data in cloud computing can be dynamically expanded, and the computer users can fully expand according to their own needs, which means that the data resources in cloud computing have considerable scalability. Fourth, the virtualization of data is promoted. Virtualization technology in the cloud computing environment is the core of this technology, which can be abstracted by using the underlying architecture, resulting that differences and compatibility between devices tend to be transparent towards the application of upper-layers, allowing the cloud to implement unified management of the underlying data. Fifth, data is implemented on demand. In the overall cloud computing, computer users can decide which cloud computing service can be used according to their own needs, and can also calculate the required cost based on the actual demand usage.

4. Analysis of the Security Problems of Big Data in the Cloud Computing Environment

4.1 Security and Privacy of Cloud Computing and Big Data

Cloud computing is a new computing method based on network information technology, and its application can further optimize the allocation of computing resources, so that resources can be more widely shared. On the basis of promoting the rapid allocation and release of computing resources, cloud computing may also cause corresponding hidden dangers to information security and network security. In terms of data storage, whether cloud platform can effectively improve data security is the focus of the whole society. Not only the cloud platform itself has a certain vulnerability, which is vulnerable to be attacked and intruded by the external world, but also some bad cloud service providers will randomly steal the user information stored in the cloud platform for their own interests, so that the data information is modified, leaked or even damaged. Big data mainly refers to the data stored by the owner of data, which has the characteristics of high growth rate, diversity and huge quantification, so it is often called mass data. In view of the development of the big data era, the big date technology are increasingly closely integrated with the daily life of modern people, so that it is difficult to protect the security and privacy of big data, which greatly affects the development and progress of the current society. At present, big data security covers the safety performances such as infrastructure, storage, network and privacy, and the corresponding data security technology is the technology of data acquisition security, storage security, mining security and publishing security.

4.2 Big Data Security in Cloud Computing

To ensure the security of big data in the cloud computing environment, not only the security of data content itself needs to be ensured, but also the information of data structure, user access history and access mode need to be protected. Usually, there are two types of security services for cloud data. One is that computer users should take the initiative to provide local data to cloud service providers for storage, management and sharing to the authorized legitimate users. The other one is that computer users implement data calculation and operation by using the resources provided by cloud service providers. Therefore, the relevant parties in society should pay more attention to the security of big data under the cloud platform, and attach great importance to the security of big data under the cloud computing platform, constantly promote the legislative work of Internet information services, and deeply explore the algorithms and protocols of data encryption and protection and apply them to practice, so as to better face the ever greater security challenges.

5. Several Ideas of Big Data Security Assurance in the Cloud Computing Environment

5.1 Introducing Data Encryption Technology

Big data security protection system in cloud computing covers many contents, such as security attributes, security location and security passwords, etc. Setting up passwords in time is a very effective way to protect existing information, and can provide the most basic protection for data. Big data security in cloud computing mainly refers to whether the data in the data life cycle in the cloud environment has enough security. Storing the corresponding information and data in a more secure environment can effectively reduce the risk of data application, and effectively avoid data steal or leakage problems. Of course, there will be corresponding security threats in data storage. Thus, the relevant data should not be stored in the encrypted protection area to ensure the security of data, and to improve the information security in storage and computing.

5.2 Strengthening Security Access Control

The so-called security access mainly refers to the access rights correspondingly arranged for data to better share the resources in a more secure system environment, and to protect the user-related data privacy by using access control. In data storage and transmission, the legitimacy of access requests should be detected, and the relevant operation process of data should be strictly controlled, which mainly covers the process of reading, querying, modifying, etc. Password management mechanism should be created, and the password control and other related operations should be used to continuously improve the new security of data. Based on cloud computing, security encryption, secret key preservation, temper-proof module and other related technologies should be better used. In the development process of big data technology, the above technologies have gradually become mature. In the future, these technologies should be improved and developed by closely combining the needs of the vast number of users. In the process of implementing security protection, the application of data mining and database access technologies is still relatively small, and new technologies of data protection can be formed in cloud computing, such as cipher-text retrieval, so that cloud computing data can be retrieved in the form of snapshot and backup.

5.3 Improving Identity Authentication Capability

With the introduction of cloud computing services, trust boundaries of data security department have evolved dynamically and have been migrated into controllable range. In cloud computing, the boundaries of network, system and applications in management organizations are extended to the scope of service providers, resulting in the decentralization of some control rights, which causes a great challenge to the existing trust management and control methods. Once the scientific and normative disposal cannot be implemented, it will greatly affect the reasonable development of cloud computing services in the institutions. Identity authentication is usually an important basis for using the infrastructure of the underlying identity, and the authentication of identity and password is implemented on the basis of saving the individual or minority user account information into ordinary documents. But this method does not apply to all systems. In order to achieve effective access, identity and computer type must be centralized to better meet the needs of multiply renters and mass identities, so the cloud computing system also needs to create a unified identity authentication and authorization system to continuously improve the identity authentication technology. Firstly, digital certificates can be used to authenticate, and hardware information binding and biometric identification can be used for the central authentication of user information. Secondly, services or domains for different users can be differentiated, and user levels can be defined according to their computer types to achieve centralized authorization of resources and access in the cloud computing system, and the fine-grained authorization can be introduced for those special users. Thirdly, the security of account number should be ensured in account management. For those accounts that are not used for a long time, they can be activated or cancelled. User accounts should be withdrawn from the

test to ensure that the same account only can be logged in one place at the same time.

5.4 Creating Virtualization Architecture

The virtualization architecture and trust architecture in cloud computing can protect the reputation of applications from malicious code. For the platform virtualization architecture in cloud computing, an application layer based on trust chain is created by using TCG extension, which can avoid the attack and destroy of virtual machine from external attackers. For the IAA-based operating system, this type of cloud service can effectively meet the needs of users for open services, but also implies that the integrity measurement of the current system does not support practical application, which should be modified and upgraded towards the current operating system to ensure the security of users. Firstly, a platform information chain should be created to ensure the secure operation of the host and to improve the trustworthiness of the host. Under this mode, a trusted authentication system can be designed in the monitor of virtual machine to improve the trustworthiness of the virtual machine. Secondly, a trusted connection delivery system can be created to reduce the risk in the start-up process by applying the security guidance of VMM and virtual machine BIOS. In this process, the most important thing is to use the trust guidance form under the guidance of multi-group order, so that all agencies can improve the security performance of data utilization according to the sequence of system control startup.

5.5 Improving Data Backup Ways

According to the strong portability feature of current mobile storage device in data security backup, so in the process of big data protection in cloud computing, full attention should be paid to the protection of mobile devices in data storage, and the problem of data omission caused by external forces in use can be effectively avoided. As long as data cannot be restored, it will cause great losses to computer users. In order to effectively avoid this situation, the backup function of data should be strengthened, and although user data can be uploaded to the cloud server to ensure the reliability of the backup, the cloud server is not completely secure in actual, so the data backup is only a planned solution. In order to create a more secure and reliable data backup system, it is necessary to ensure that the user terminal is well prepared for data backup, and use cipher-text transmission in backup transmission to ensure security.

6. Conclusion

In summary, although cloud computing is the main method of big data processing in the current situation and has generated great convenience for data processing, there are still come security holes which cannot be ignored. To this end, this technology should be viewed accurately and should be continuously improved and perfected, so that it can truly benefit all kinds of people, thus promoting the continuous development of the information level of modern society.

Acknowledgement

This work was supported by 1.College-level Project of Xi’an Peihua College, "Research on Dynamic Migration Algorithm of OpenFlow Switch Based on Attractor Selection in Cloud Environment", No. (PHKT18062); 2. Project of Education Science Planning in Shaanxi Province in 2017, "An Empirical Study on the Teaching Reform of Computer Application Foundation Course Based on Systematization in Working Process under the Background of Transformation and Development", No. (SGH17H461); 3. 2017 Special Science and Research Planning Project of Education Department in Shaanxi Province, "Research on Location Algorithm of Wireless Sensor Networks Based on IR-UWB Technology", No. (17JK1059).

References

[1] Song Wenchao, Wang Ye, and Huang Yong. Model Simulation for Intrusion Detection of Cloud Computing Network under Large Data Environments, *Science and Technology of West China*, 2015(8).

[2] Wu Hongjiao. Privacy Protection and Data Security in Cloud Computing, *China New Telecommunications*, 2015(17).

[3] Tian Yongmin. Research on Big Data Security and Privacy Protection in Cloud Computing, *Electronic Technology & Software Engineering*, 2016(13).

[4] Li Hongyan. Discussion on Data Security in Big Data Cloud Computing Environment, *Communication and Computer (Theoretical Version)*, 2017(3).

[5] Zhang Xueya. Research on Security Access Control Mechanism of Data Stored in Cloud Computing, *Computer Measurement & Control*, 2018(5).