Risk Analysis and Strategy Research of Information Security under the Environment of Cloud Computing

Xueli Wang

Jilin University of Finance and Economics, Changchun, Jilin province, 130117, China

Keywords: Information security, Cloud computing, Privacy leakage

Abstract: The development and application of cloud computing technology have brought tremendous changes to the development of modern society. More and more individuals, organizations and governments have adopted this advanced service model. But the information security risks of cloud computing is a problem that cannot be ignored. The problem of false information, leakage of user privacy and imperfection of security technology are all important factors affecting information security in cloud computing environment. From the perspectives of the government, cloud computing service providers and users, this paper gives the response strategies of information security risks in cloud computing environment to provide some references for the relative researchers.

1. Introduction

Cloud computing, after the launch of the National Institute of Standards and Technology, has a high degree of recognition in the industry [1]. Cloud computing can access configurable computing resources according to actual needs. This computing resource includes servers, networks, applications, storage devices and related services. Generally speaking, cloud computing has five essential characteristics: extensive network access, on-demand self-service, fast resilience, resource pool and measurable services. In recent years, with the rapid development of computer and network technology, cloud computing as a new technology has been widely used in the world. It can handle the data of various industries well, and provides convenience for people to store and calculate data. Because cloud computing has the characteristics of low cost and high flexibility, many traditional basic services are deployed on the cloud service platform. Cloud computing can carry out large-scale distributed computing in the network, people do not need to worry about insufficient storage space, do not need to obtain huge storage capacity and computing resources to invest in expensive hardware and software costs, saving users energy and costs. Cloud computing effectively promotes the development of network technology, improves the integration of various data, and strengthens the communication between the Internet terminal devices. Although cloud computing technology can ensure the security and reliability of information to a certain extent, it belongs to the emerging network technology after all, inevitably there will be some information security problems. Cloud computing is characterized by storing user data in the cloud, separating data management rights and ownership, so that users can not directly control the data, all user data will be managed by the cloud platform. It is this data management model of cloud computing that can lead to illegal access, malicious tampering and disclosure of cloud resource data by cloud administrators. Cloud computing greatly facilitates users to obtain information, but it also brings greater information security risks than the previous information technology [2].

2. Information Security Risk under the Environment of Cloud Computing

2.1 Problem of False Information.

At present, China's computer user base is huge, and its complex identity makes the network

  DOI: 10.25236/iccse.18.055

environment very complex [3]. The application of cloud computing technology increases the exchange and sharing of information and data, and promotes the spread of false information in the network. False information and false network address pose a serious hidden danger for computer network security. Because the current development of cloud computing technology is mainly aimed at the perfection of its own functions, the lack of computer protection system construction, the existence of vulnerabilities in user addresses and network resources, resulting in false information and destructive information under the promotion of cloud computing technology to achieve a wider range of interference, resulting in many losses for users. It has further hindered the application of cloud computing technology. The security of application layer should be the key to the safety of the whole infrastructure. Open source is the soul of cloud computing, and the biggest vulnerabilities in open source network applications include execution of malicious files, script injection, and bugs caused by programming errors. Hackers will constantly scan these network applications to grasp these vulnerabilities for intellectual property theft and network fraud. This not only poses a threat to cloud computing service providers, but also increases the risks and losses faced by users. Basically, existing network programs have security flaws such as incomplete access verification mechanism, programming logic errors, etc. For cloud computing service providers, their network applications built on public cloud platforms must withstand Trojan horse, virus and hacker attacks. Once the outsourcing companies have technical disasters or business problems, the security of information cannot be controlled.

2.2 Leakage of User Privacy.

Cloud computing is a marketing model that provides services to users through the Internet. It connects a large number of individual computer users through specific data and port technology to configure computer resources in cloud computing. In this process, a large number of information resources are closely linked, making the client information more transparent, easy to cause information leakage, and bring losses to users. In addition, network information leakage not only brings losses to users, but also may lead to serious social problems, affecting the development of a harmonious society. When users use cloud computing services, they do not know which specific hosting server the data used belongs to. When cloud users and cloud service providers use cloud computing services, data loss and data theft security problems inevitably arise. From the perspective of data security, we can start with data privacy and data isolation. Software as a service provider has the ability to process sensitive data, which other vendors do not have. Sensitive data is also privacy data. Data sharing in cloud computing services has the characteristics of data sharing, but users do not have an independent storage area, a lot of potentially dangerous data is difficult to attract high attention of users, especially in cloud services, LAN data access risk and benefit assessment methods also have good applicability. Cloud computing is different from traditional software. Data maintenance does not rely on third-party maintenance, because cloud computing architecture data has the characteristics of decentralized storage, and have plaintext storage features. Although firewalls can be used as a form of protection, they still reveal some key data, so the implementation of flexible computing process and data privacy protection can be achieved by building a private cloud and building a hybrid cloud [4].

2.3 Imperfection of Security Technology.

At present, the development of cloud computing network service system in China is still imperfect, there are still big problems in information protection, cloud computing technology in the provision of some depth of service is very poor. China is a country with a large population of computer networks. If cloud computing resources carry huge and complex applications, it will bring tremendous impact on computer network security and defense. Once loopholes occur, network information security system will be greatly hit, and then information leakage and information destruction will occur. In addition, the development of computer technology has also promoted the progress of hacker technology, more and more illegal elements use hacker technology to damage the computer network environment, become an important aspect of network security under cloud computing. In the

application of security technology, besides strengthening the traditional security technology, such as firewall technology, anti-virus technology, intrusion detection technology, data encryption technology, identity authentication technology, monitoring and auditing technology, disaster recovery and backup technology, we should also develop more targeted security technology according to the characteristics of cloud computing, such as homomorphic encryption and its corresponding cipher text retrieval and processing, accountability, virtual security technology, trusted cloud computing, generally speaking, the higher the degree of localization of technology and equipment, the higher the information security coefficient. Therefore, the key to ensure cloud security is to achieve self-control, domestic technology and equipment shoulder the major mission of cloud security. Cloud computing ecosystem includes six major roles: cloud device providers, cloud system builders, Cloud Application developers and cloud service operators, cloud service deployment, cloud service vendors. Among them, cloud service providers are directly related to users. When it provides services to users, it also needs to purchase the other five roles of the corresponding services. This kind of multi-layer subcontracting service, the "short board effect" is very obvious, whether the coordinated development is crucial.

3. Response Strategies of Information Security Risk under the Environment of Cloud Computing

3.1 Strategy of Government: Information Security Legislation.

The government's relevant legislation on cloud computing security should be able to meet the actual needs of cloud computing industry and users, ensure that it can promote the healthy development of the national cloud computing industry, and provide comprehensive services and guidance for the national cloud computing industry, amend the backward and inadaptable legislative concepts for the development of modern industries, and trust Information security legislation from a simple "control" to cloud computing information security clearance development barrier, the formation of cloud computing information security for the actual needs of the rule of law culture. When providing cloud computing services, American companies cannot ensure that users' information is not accessed by the US government. Overall, the legal policies applicable to cloud computing in the United States are both committed to and give the government the right to access data. I think it is important to find a balance between user data security and government information security. To strengthen the foresight and efficiency of cloud computing security legislation, cloud computing security laws and regulations should not be passive and lagging behind. The role of laws and regulations in the maintenance and construction of cloud computing security should also be reflected in the forward-looking and active standardization of cloud computing development. When formulating laws and regulations, we should pay attention to conform to the characteristics and special requirements of cloud computing technology development, and eliminate the possibility that relevant laws may bring obstacles. Cloud computing is based on the Internet, and the internationalization of cloud computing service providers and the globalization of service users make it possible and necessary for the relevant legislation of cloud computing information security to be in line with international standards. When formulating policies and laws and regulations, China should pay special attention to compatibility with existing international rules, and should participate more in the creation and establishment of international rules in order to safeguard China's international interests. The government's leadership and management are to ensure the reliability and authority of the third party regulatory bodies. In addition to monitoring and management, third-party regulators can also audit and evaluate cloud computing providers.

3.2 Strategy of Cloud Computing Service Providers: Technology Innovation.

The key to solving the security of physical environment is to design and maintain a secure external hardware environment to prevent unauthorized access, damage and interference to equipment and buildings. This involves the design and control of external security boundaries and entries. For data

loss caused by physical layer risk, the service provider should establish data disaster recovery system, adopt data redundancy, remote storage, establish two or even more sets of the same cloud computing system in two places far away, ready for monitoring and switching between systems at any time, when one of them stops working because of an accident and the other. The system is switched to work in time to maintain the normal operation of cloud computing services, and can provide a backup of unexpected node data, and can be restored. Cloud computing service providers send applications directly to users, whose permissions are simple access and operation, so they are responsible for the security of applications and components when developing applications. PaaS security issues focus on the client side, especially in the PaaS service mode is becoming more and more popular, these malicious attacks are more likely to penetrate the cloud computing service provider platform through the network, and cloud computing service providers are facing tens of thousands of customer nodes, which means that the service providers are not only With huge service requests, it will make the cloud computing service platform very fragile. PaaS mode services need to be accessed through the browser. First, the security of the access platform should be designed, and secondly, the security of the network program should be established on the browser platform. The best way to do this is to use user authorization and single sign on.

3.3 Strategy of Users: Cultivation of Information Security Consciousness.

Judging from the disclosed and reported leaks of cloud computing information, a considerable part of user information is destroyed by loss or theft of personal information related to themselves, such as their birthday, telephone, bank account, password stored in the cloud computing server or as a server login user name. . From this point of view, besides the immature security technology and large system vulnerabilities adopted by cloud computing service providers, the lack of user information security awareness and literacy is also an important factor. Good information security literacy includes the awareness of information security, information security knowledge, information security capabilities. A good sense of information security includes understanding the current form of information security and facing threats and challenges. Understand and appreciate the decisive factors in the process of information security. Good knowledge of information security includes the latest information on the latest viruses and Trojan horses. Understand the basic knowledge of information security technology. Data encryption is still the most reliable and effective way for information system to protect information. It uses cryptographic technology to encrypt the information, to achieve information concealment, thus playing a role in protecting the security of information. The user encrypts the information and saves the key before transferring the data to the cloud computing service provider. Know the basic rules of information security. Information security capabilities include: protecting the safety of physical devices. Set the password that does not leak information with itself. Regularly backup important information and encrypt it. Users of cloud computing services should avoid using login names and passwords related to their identity. Know the laws and regulations on information security and take the initiative to take legal measures to safeguard their rights and interests after the occurrence of information security problems. It is best to take encryption measures to save important information and keep it back in time.

4. Conclusion

Information security in cloud computing environment requires the participation of users, cloud computing service providers and relevant national managers. Users should constantly enhance their knowledge of cloud computing security awareness, using the right channels under the cloud computing operations and management. Cloud computing service providers should provide users with safe and effective cloud services, correctly identify user information, ensure the security of user information in the cloud computing environment, and avoid stealing user information. According to the development direction of cloud computing, the national managers should establish more perfect standards for the development of cloud computing in all walks of life as a guide to build a relatively safe cloud computing environment.

References

[1] Zhou Jian. Research on information security under cloud computing background [J]. Modern Electronics Technique, 2017, 40(11): 84-87.

[2] Wang Xiaoni, Han Jiangang. Research on Information Security Threats and Defense Strategies of Cloud Computing [J]. Aeronautical Computing Technique, 2018, 48(2): 113-117+121.

[3] Wei Guangxi. Personal Information Security Risks and Prevention Measures in Cloud Computing Era [J]. Journal of Chongqing University of Technology (Social Science), 2016, 30(2): 92-97.

[4] Gao Yuan, Wu Chang'an. Study of Informational Security Question under the Cloud Computing [J]. 2015, 33(11): 48-52.