Research on Network Security and Defense Strategy in Cloud Computing Environment

Wang Xiaoni

***Abstract*—With the arrival of the era of information and big data, cloud computing has been widely used as a new computer network technology, and it has a good prospect. Cloud computing technology for our information storage and data computing is facilitated, but there are also network security risks. This paper deeply studies the network security problems in the cloud computing environment, and carefully discusses the cloud computing network security issues of defense solutions. This scheme can effectively solve the network security risks of cloud computing by comprehensively defending the four aspects of state, cloud computing users, R&D personnel and suppliers.**

***Index Terms*—Cloud computing, defense strategy, network security.**

I. Introduction

Cloud computing technology is a new network technology with the development of Internet technology and computer, and its presence makes calculation and data storage very convenient. Cloud computing allows carrying out large-scale distributed computing in the network. People don't need to invest in high hardware and software costs to get an oversize storage and computing resources, saving their energy and cost. Cloud computing has effectively promoted the development of network technology, improved the integration degree of network data, and strengthened the communication between the terminals of the internet. Although cloud computing can guarantee the security and reliability of the information in a certain extent, it is a new network technology after all, and some network security problems will inevitably appear. With the rapid development of Internet and Cloud computing technology, network security is facing serious problems. For example, DDos attacks, prism events and Struts vulnerabilities in 2013; Ctrip's "security gate" incident and Openssl heart bleeding loophole in 2014; GHOST ghost loopholes and NetEase mailbox data leak events in 2015; In 2016, the United States suffered DDos attacks and Hillary mail door events; In 2017, the extortion virus WannaCry swept the world and hackers invaded Yahoo's user account, etc. They have a serious impact on network security. In order to build a good network environment and promote the development of cloud computing technology, it is urgent to optimize the computer network security technology.

Manuscript received February 29, 2018; revised May 12. This work was supported in part by special research fund project of Xianyang Normal University under Grant 13XSYK087.

Wang Xiaoni is with the Xianyang Normal University Information Center, Xianyang city, Shaanxi province, China (e-mail: wxnhjg1@ 163.com).

II. Cloud Computing and Network Security

A. Concept and Characteristics of Cloud Computing

Cloud computing is a commercial computing model developed on the basis of electronic communication, Internet and computer technology [1]. It is the product of the development of network technology and computer technology, such as distributed computing, utility computing, parallel computing, virtualization, network storage, load balancing and so on [2]. It is distributed in the resource pool computing tasks, so that all users or applications can be based on actual needs for the computer or network terminal equipment to provide the appropriate storage space, information data, computing power or hardware and software resources, in order to achieve a range of fast and convenient resources shared. Cloud computing technologies such as cloud storage, distributed processing and virtualization technology have greatly reduced costs. Cloud computing has these five characteristics: on-demand self-service, extensive network access, resource sharing, rapid scalability and measurable services [3].

B. Application Model of Cloud Computing

The application model of cloud computing consists of deployment model and service model [4].

1) Deployment model

According to NIST definitions, cloud computing can be deployed on the four types of public cloud, community cloud, private cloud, and hybrid cloud [5].

- Public cloud. In a public open environment deployment, the core components come from the infrastructure of cloud computing service providers. Only users or systems that can access the Internet can enjoy services, but these users have only the right to use, not to manage and possess.
- Community cloud. It is also called the agency cloud, deployed in a relatively open environment, software and hardware and network services from multiple cloud service providers such as infrastructure, according to a certain agreement to complete the user resource sharing, and to provide users with the same focus of community service.
- Private cloud. It is deployed in a specific closed environment, with a clear system boundary, belonging to large institutions, and provides services for privileged users.
- Mixed clouds. It is also called heterogeneous cloud whose deployment environment is relatively complex and consists of various forms. It is composed of a plurality of independent cloud. It uses the cloud interoperation interface to implement applications, network information, and data portability.

doi: 10.18178/jacn.2018.6.1.251

2) Service model

Generally, the structure system of cloud computing is divided into two parts: cloud user and cloud provider according to the base cloud hierarchy [6], as is shown in Fig. 1. Specific subdivision is user access layer, resource layer, application layer, platform layer, management. The cloud computing service model consists of these three components [7].

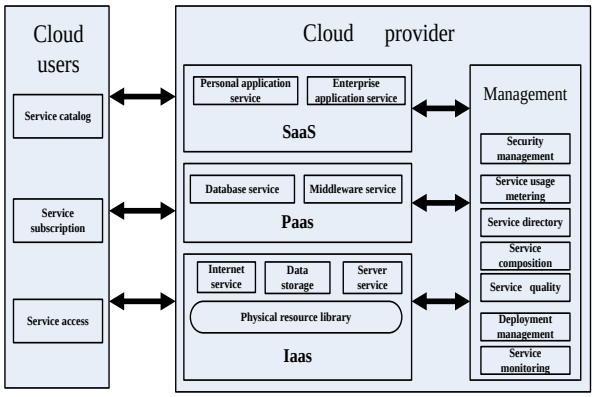

Fig. 1. Architecture diagram of cloud computing.

(1) IaaS (infrastructure as a service). it provides users with infrastructure services to compute network and store integration. It centralized scheduling and management of communication equipment, computer hardware and network storage and other infrastructure in the cloud computing system. It encapsulates these infrastructures in a particular way and ends up with infrastructure services.

(2) PaaS (application platform as a service). It uses the internet to provide users with an application software support platform for the development, operation and operation of the application software on cloud computing infrastructure.

(3) SaaS (software as a service). It provides software services for users on the cloud computing platform using the internet. Users do not need to purchase and maintain software, they don't have to invest too much in R&D teams and hardware and software too. Users only need to pay the right amount of rental fees so that they can use the appropriate service through the Internet.

3) Network security and its importance

A common definition of Network security [8]: It refers to the protection of data in the hardware, software and system of the network system. The system runs continuously, reliably and normally without interruption due to accidental or malicious reasons. In a broad sense, computer network security mainly includes key technologies such as security management, password, security audit, authentication, firewall, host security and access control. Now computer network security is not a potential problem, but an very important problem in information society. It is related to national politics and security, involving the military lifeblood of the state, affecting the sovereignty and stability of the state. It is not only the research focus of the people in the field of technology, but also of the countries, governments and businesses.

III. The Problem of Computer Network Security in Cloud Computing Environment

Cloud computing is a great way to separate virtual services from real physical resources, reducing the burdens of various services and improving the utilization of network resources [9]. With the continuous advancement of cloud computing research and application both at home and abroad, cloud computing has penetrated into every corner of our lives, and its security has attracted the close attention of scholars and users. As a new network technology, the security of cloud computing has become one of the core problems in cloud computing. For example, Norton Cybercrime Report 2011 [10], the total amount of losses caused by global cybercrime has reached an astonishing $ 388 billion, far greater than the total sum of cannabis and heroin illegally traded around the world. Thus, it is very important to strengthen the network security in the cloud environment. At present, cloud computing still exists these network security issues.

A. Imperfect Cloud Computing Network Security Management System and Related Laws and Regulations

In the cloud computing environment, there are many information data about leakage, tampering and stealing of users in China. The essential reason is the lack of laws and regulations on protecting information data and the perfect legal system of cloud security management. Cloud computing is in the midst of a rapid development period, constantly improving the openness of the network and facilitating the rapid sharing of data resources. However, there is no common development of network security regulation and legal system related to cloud computing. Some areas are even absent from the legal system. On the issue of cloud security, the country lacks specific legal provisions, and the penalties for illegal attacks and hackers are weak. This leads to the difficulty of enforcing the law and the risk of leaking user data when dealing with network security problems.

B. Related Personnel's Weak Network Security Awareness in Cloud Computing

Cloud computing has low requirements for client devices and users. As long as it can connect to the network, you can access the application provided by the provider through the browser, which has a network security risk [11]. Some users may just go online and don't understand the security of the Internet, but the access data doesn't matter at all. This kind of user network security knowledge is poor, prevention consciousness is weak, Internet habits are bad. They do not know how to choose a reliable cloud computing vendor. They will not install anti-virus software on their client devices and keep their own authorization information. Ordinary users cannot correctly identify the false addresses and tags in the cloud computing network, resulting in the failure of cloud computing to run correctly, which facilitates the attack of criminals.

C. Laggard Network Security Technology of Cloud Computing

Although the computer information technology has made great progress and development, but the stability of the network is not optimistic. The core technology of cloud

computing is virtualization, which makes the data sharing boundary is not obvious, resulting in failure to ensure user data security. Network interrupts occur frequently, which can lead to server or network service failure, and make the data on the server unable to process and obtain, which directly results in the failure of cloud computing in network data storage or computing operations. At present, due to the lack of good measures to deal with the phenomenon of network instability, once the network is interrupted, cloud computing users will be passively damaged. As masters of network technology, hackers are more skillful in technical application than technical engineers, using illegal authorization to illegally run cloud computing [12]. Therefore, the key problem of cloud computing technology application is how to ensure the secure and reliable transmission of information data? It is necessary to strengthen the research and development of network security technology in cloud computing environment.

D. Poor Reliability of Suppliers

Only reliable cloud providers can ensure user data security, but there is a lack of detailed criteria for evaluating suppliers' credibility. If the user chooses an unreliable cloud computing provider, the system he provides deploys a cloud service that is not standardized in the design scheme. Therefore, there are some hardware and software defects and security risks in operation, which are used to facilitate hacker attacks. If the provider lacks integrity, then there is an internal security hazard in the cloud computing. Therefore, the managers of cloud computing providers can use their work to make illegal operations, and it is easy to steal data stored in the cloud computing server and transmit it.

IV. DEFENSE STRATEGY OF CLOUD COMPUTING NETWORK SECURITY

A. Conceptual Design

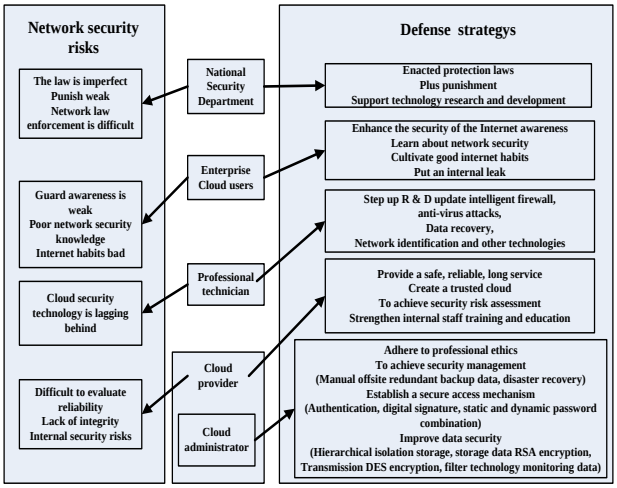

Fig. 2. Cloud computing network security solutions.

According to the previous analysis, cloud computing is faced with these four aspects of security issues: imperfect safety management system regulations, weak safety awareness of relevant personnel, outdated cloud computing network security knowledge and poor reliability of suppliers. In view of these cloud computing security risks, combined with the current actual situation, research and design a specific feasible solution, as shown in Fig. 2. The scheme is to solve the network security problems faced by cloud computing from five aspects, such as the national regulatory authorities, related personnel in cloud computing and cloud providers.

B. Programmer Implementation

The solution of network security problem in cloud computing environment is implemented from the following four aspects to ensure the security of user data. First, the national security administration should improve the legal policy and management system of cloud security. Secondly, enterprise cloud users and managers should enhance their awareness of prevention. Then the network technician should strengthen the professional technical research and development of this aspect; Finally, cloud providers need to improve their reliability.

1) Improve the legal system for cloud security management

Due to lack of laws and regulations on cloud computing network security, there is no complete network security protection system. Therefore, cloud computing application service system collapse; user information theft cases are common. Therefore, the national information security department must take necessary measures to solve the network security problems of the current cloud computing, and introduce relevant laws and policies to make up for the shortcomings of the existing legal policies[13]. Limit the illegal practices that ravage rampant cyber security and user data. We should increase the punishment of hackers on Internet Illegal attacks, protect the legitimate rights and interests of authorized users, and establish a harmonious cloud computing network environment. At the same time, the government departments should formulate relevant incentive policies to support and encourage the research and development of cloud computing network security knowledge professionals [14].

2) Enhance the network security awareness of relevant personnel of cloud computing

In the cloud computing environment, users face various complex network security problems. In order to better adapt to and use cloud computing technology, the network security awareness of relevant personnel must be established and enhanced.

(1) General enterprise cloud computing users. In the face of the network security knowledge level of enterprise cloud users, enterprises should be able to increase publicity and provide training opportunities. Let all users have a comprehensive understanding of network security problems in cloud computing environment, raise awareness and correct operation, and reduce the occurrence probability of unsafe events. Only all users realize the importance of network security, so as to reduce the risk of network. In the complex cloud computing network security, users are required to take defensive measures from these four aspects: Firstly, Enhance the security awareness [15]. In the process of accessing cloud services or surfing the Internet, you should keep your authorization or authentication information properly, pay

attention to the password with high complexity and change frequently. Don't store your personal information or account information on your own terminal equipment, and don't spread it online. When using cloud computing for information processing, users should be far away from the use of public WiFi accounts in the external network or public places. Don't use other people's devices to access, deliver, and share personal system information on the cloud platform. Log in timely after login information. Unsafe applications or websites cannot be accessed. Don't open unknown sources of mail or links. Download software through a reliable website. Beware of Trojan horse virus and network fraud. Secondly, Continue to acquire network security knowledge. Keep abreast of the latest network security information, accumulate network knowledge, familiarize yourself with the use of network terminals and cloud computing applications, such as browser compatibility and security level settings. Thirdly, Cultivate good Internet habits and pay attention to the protection of personal terminal equipment information. For all of the Internet terminal equipment, cloud security function antivirus software should be installed and checked on time with regular comprehensive vulnerability scanning and virus library upgrade. Because each anti-virus software has its own characteristics, it should be used in combination with its advantages and disadvantages, so it is better to install compatible or frequently different antivirus software. Avoid unauthorized access by unauthorized users or view your own terminal devices. The sensitive or important personal data should be regularly arranged, and get timely and manually redundant backup so as to be convenient for the data recovery when disaster occurs. Users have to encrypt the privacy data before they can upload and store it to the cloud computing system server. Fourthly, Select reliable cloud computing vendors. At present, there are many providers of cloud computing, providing different types of services. The quality of cloud services offered by different cloud providers varies greatly. In order to prevent the user's important information data is stolen, users should combine their own specific requirements for cloud computing services, to study from many angles, try to choose well-known service providers, credit honesty and high reputation. In general, such suppliers have the strength to provide a stable system, professional technical staff and strong data security protection measures.

(2) Cloud computing professional managers. On the basis of ordinary enterprise users, the cloud administrator must also do the following technical protection, to ensure data security and confidentiality. Firstly, strictly abide by professional ethics and prevent internal leaks from security risks. Secondly, implement security management proxy server and application. According to the user's business requirements, the user level and access rights are appropriately divided. The cloud administrator is divided into ordinary maintenance personnel and core operation administrator. General maintenance personnel access to general data operation management. They are responsible for the security of applications and operating systems to protect them from threats and vulnerabilities. They do routine maintenance of data, but they can't operate confidential data directly. The core manager can operate all the data, but they have to follow certain rules and processes. Thirdly, establish security access mechanism. Continuously improve the user's identity and access control services. The administrator adopts real-name system, authentication and digital signature technology to control the access of user. All users must not have the same authentication information. For user authentication, increase the variety of processes and links. Administrators need to use the fingerprint, dynamic and static password of user combination, in order to achieve a full range of user information authentication. When a user accesses a cloud computing server system data, the user must first authenticate and complete the correct digital signature through legal authentication. Fourthly, improve data security. ① Data storage. In optimizing the storage structure of the data [16], the administrator stores all the data information according to the type, separates from each other. Use the general data for the cover, the administrator first makes confidential data have address masquerading, and then stores these data scattering in different parts of the network database, so easy to data disaster recovery. ② Data encryption. The administrator uses RSA and DES to encrypt the user data, which can save cost and improve efficiency. The administrator uses ESD encryption technology in the process of transmit data [17]. The asymmetric data (file or key) stored at the client and server side is encrypted with RSA. The user must use the private key. ③ Real-time monitoring. The administrator adopts the filter technology (Websense or Vericept) [18] to monitor the user's remote operation and data transmission process, and timely intercept and filter suspicious data or illegal sabotage.

3) Strengthen the development and application of cloud security technology for network technology personnel

With the rapid development of cloud computing technology, various kinds of cyber attacks and viruses are emerging, which requires the Internet security technology to keep up with the times. However, because China's cloud computing technology is currently in the primary stage, the network security infrastructure construction lags behind, and the security flaws in the technical aspects need to be improved. This requires our professional and technical personnel to continue to strengthen (intelligent firewall, data encryption, anti-virus [19], data recovery and network identification, etc.) network security technology research and development and application. Attention to cloud computing network security technology research and development, we can effectively guarantee the scientific health of the harmonious network environment construction This is also the key to the progress of cloud computing technology in China, which is essential for our country to be among the world's forefront in this field.

4) Cloud computing providers provide reliable cloud services

(1) Improve the integrity and quality of service. Cloud providers use filters, VPN, data encryption, authentication and other technologies to implement cloud computing architecture security. Cloud providers combine multiple authentication methods to avoid the emergence of user information security vulnerabilities.

(2) Create trusted cloud. Cloud providers use trusted algorithms to build trusted relationships from the bottom to the top in cloud computing systems, and build trusted clouds. Cloud providers use distributed computing security and

virtualization technologies[20] to provide reliable cloud computing for users.

(3) Implementation of security risk assessment. The cloud provider sets its own security service level to assist users in assessing their own applications and data. This is the basis for providing the user with a level of service.

(4) Strengthen the safety of internal staff education and training. The cloud provider should strictly regulate the internal staff, improve the internal organization[21], and eliminate the disclosure of authorized user information.

V. Conclusion

There is a lot of data exchange between cloud computing platform and enterprise cloud users, and all the data storage and transmission face security threats. This paper analyzes the cloud computing and its security issues in depth, and puts forward the feasible cloud computing network security solution. Through the national security management departments, professional and technical R & D personnel, cloud computing providers and enterprise cloud users to work together to take appropriate measures to form a comprehensive cloud computing security protection system. Practice has proved that this program not only to provide users with better service, but also to promote the cloud computing technology to better benign development.

References

[1] L. Juyin, "Network security issues and countermeasures in cloud computing environment," *Communication World*, vol. 9, pp. 15-16, 2015.

[2] M. Xiangkun, "Cloud based network security event detection," Master's dissertation, Tianjin University of Technology research, 2014.

[3] H. Shuai, "Research on key technologies of data security based on cloud computing," Master degree thesis, University of Electronic Science and Technology, 2012.

[4] W. Stallings, *Network Security Essentials Applications and Standards*, 5th ed. Beijing: Tsinghua University press, 2014.

[5] L. Ming, "Research on identity authentication and service access security in cloud computing," Master's degree thesis, Huazhong University of Science and Technology, 2012.

[6] R. Tao, "Cloud computing security solution scheme," Master degree thesis, Central South University, 2012.

[7] L. Deng, *Cloud Computing Foundation and Application*, Beijing: Mechanical Industry Press, 2016.

[8] Y. Jinsheng and W. Yannong, *The Basis Of Computer Network Security*, 4th ed. Posts and Telecommunications Press, 2013.

[9] Z. Weiwei, "Research on data transmission and storage security solution for cloud computing," Master's thesis, Beijing University of Posts and Telecommunications, 2011.

[10] NortonCybercrimeReport2011[DB/OL]. [Online]. Available: http://www.symantec.com/content/en/us/home_homeoffice/html/ncr

[11] H. Yongfeng, "Talking about computer network security in cloud computing environment," *Journal of natural science of Harbin Normal University*, vol. 1, pp. 63-66, 2015.

[12] L. Tingting, "Research on Key Technologies of data security protection for cloud computing," Doctoral dissertation, Information Engineering University, 2013.

[13] "Research on information security protection scheme based on cloud computing," *Automation of Manufacturing Industry*, vol. 34, no. 5, pp. 113-115, 2012.

[14] L.Yuan, "Several issues of network security in cloud computing environment," *Technology and Market*, vol. 24, no. 9, pp. 157-158, 2017.

[15] G. Qing, G. Qing Zhuan, and J. Na, "Computer network security issues based on cloud computing environment," *Computer Knowledge and Technology*, vol. 13, no. 11, pp. 22-23, 2017.

[16] Z. Jing, "Optimization of computer network security technology based on cloud computing environment," *Journal of Career Academy, Jiamusi*, vol. 176, no. 7, pp. 436-437, 2017.

[17] Z. Shuai, "Cloud computing environment analysis, computer network information security technology optimization," *Biotechnology and Computer Science Research*, vol. 176, no. 7, pp. 433-435, 2017.

[18] Y. Zhi Shang and D. Rui, "Under the cloud computing environment of computer network security technology," *Computer Knowledge and Technology*, vol. 35, no. 12, pp. 59-60, 2016.

[19] Z. Fengqi, "On the cloud computing environment of computer network security," *Chinese Cable*, vol. 7, pp. 819-820, 2017.

[20] T. Erl and Z. Mahmood, *Cloud Computing Concept, Technology and Architecture*, Beijing: Mechanical Industry Press, 2016.

Wang Xiaoni was born in Xianyang, Shaanxi province in December 1977. In June 2011, she received a master's degree in computer science and technology from xi 'an university of electronic science and technology. The author's major field of study should be computer application and network security.

The author is mainly engaged in campus network information security and application system maintenance. In 2017, the author participated in the training of network information security technology held by Tsinghua University, and passed the "certificate of graduation certificate of Tsinghua University" and "vocational technical certificate" of the ministry of industry and information technology. The title is an engineer.

The author presided over the Xianyang Normal University Campus Fund Project 1, published more than 12 papers, 1 papers in core technology. Recently, published papers follow as:

[1]Wang Xiaoni. Analysis and Implementation of ARP Attack Defense Strategy in the Local Area Network of Campus [J]. Aeronautical Computing Technique, 2017, 47(3):125-129.

[2]Wang Xiaoni. The Design and Implementation of College OA System Based on MVC [J]. SOFTWARE ENGINEER, 2014, 17(12):36-37.

[3]Wang Xiaoni. Research and development of OA document circulation system based on workflow [J]. Computer Knowledge and Technology, 2014(32):7818-7819.