The realization of network security technology based on cloud computing environment

Wentao Yan, Sai Wang, Chengyuan Wang
State Grid Shandong Electrice Power Company, Jinnan, Shandong Province, 250001, China

Abstract. Cloud computing takes the network technology, virtualization technology, and distributed computing technology as the foundation. The business model of cloud computing is based on its own need and has formed a new application mode with the characteristics of dynamic extension, resource sharing, and others. The cloud computing environment refers to the integration of terminal devices, such as computers distributed on the Internet, to realize hardware and software resources by means of some kind of network calculation. The basic components include the application layer, platform layer, resource layer, user access and management, and technology and take all kinds of cloud computing services as the core. Under such an environment, the user's data and resources in cloud computing are wholly dependent on the unreliable network communication and partially trusted cloud storage server, which makes the users question the safety of the cloud computing environment, and resulting the arrested development of cloud computing. In this paper, network security risks and current common computer network attack method in cloud computing environment were discussed in detail and the network security protection technologies were proposed to improve the security of network of cloud computing environment.

1. Introductions
In the development of modern society, computer technology and network communication technology have become an important symbol of the information age. In recent years, China's network and information technology develops widely and rapidly, to further expand the degree of openness, sharing and interconnection, the modern computer network in the social life in various fields. Computer network technology has become the main media of the modern enterprise office and communication mode. Cloud computing will be the application of traditional computing resources integration to form the cloud service center whose capacity is bigger and faster. Cloud computing is based on virtualization technology and takes the network as the carrier, to provide the infrastructure (IaaS), platform (PaaS), software (SaaS) and other services, and to integrate large-scale scalable computing, storage, data, application to work together on the distributed computing resources such as super computing model. The application of cloud computing can expand and contract, so that users can obtain resources suitable for their own needs and improve the computational efficiency while greatly saving the cost of user accounts. Open network environment provides powerful computing and storage capacity, and has been gradually applied in industry widely. The concept of cloud computing is proposed by Google, which is a beautiful web application mode. The definition of cloud computing refers to the delivery and usage mode of IT infrastructure, which means to obtain the required resources by means of the network. Generalized cloud computing refers to the delivery and usage patterns of services, which refers to obtaining the required services through the network in an on-demand and scalable manner. This service can be IT and software, Internet related, or any other services. Cloud service is closely related to cloud
computing, by making the calculation of distribution on a large number of distributed computers, rather than the local computer or remote server, the operation of the enterprise data center will be more similar to the Internet. It enables the enterprise to switch the resources into different applications based on their needs and access computer and storage system according to demand. This kind of service type is to mobilize the network of various resources, service for the users; Since Mr Obama took office, cloud computing has achieved rapid development. For example, the amazon web services (AWS) is very popular now, and ArcGIS10 cloud service is based on the amazon web services. The development of global cloud computing is extending from the Internet to other traditional industries, and China is no exception. The policies released in 2015 paved the way for the expansion of cloud computing to industry. "Article 5" proposed the technology, industry and policy foundation that cloud computing needs to extend to industry. In terms of technology, the security and reliability of cloud computing technology is an important prerequisite for the further promotion and security of cloud computing in various industries. "Article 5" proposed to promote cloud computing capacity for independent innovation and to strengthen the basic research, the applied research, the technology research and development cloud computing related. Cloud computing is to promote safe and reliable products and solutions in all areas of application. From the perspective of industry, the enhancement of cloud computing service capability and the establishment of industrial ecology are the basis for cloud computing to be applied in the industry field. " Article 5" has also put forward the mission to enhance the capacity of cloud computing service by developing all kinds of public cloud services to fully satisfy the business enterprise, government and industry department for information resources needs at different levels, in order to cultivate the new forms, new pattern. From the perspective of policy, the regulation and policy environment adapting to industrial development is the basic guarantee for the application of cloud computing industry. In terms of policy, "Article 5" puts forward some considerations on market management, privacy protection, tax support and security guarantee.

However, along with the rapid development of cloud computing technology, its security issues faced by growing. As the computer network develops, the problems of mail bombs, hacking programs and remote listening are gradually highlighted, which seriously affect the security of computer networks. The cloud computing environment refers to the integration of terminal devices, such as computers distributed on the Internet, to realize hardware and software resources by means of some kind of network calculation. The basic components include the application layer, platform layer, resource layer, user access and management, and technology and take all kinds of cloud computing services as the core. Under such an environment, the user's data and resources in cloud computing are wholly dependent on the unreliable network communication and partially trusted cloud storage server, which makes the users question the safety of the cloud computing environment, and resulting the arrested development of cloud computing. Moreover, currently cloud computing is mainly used in large data computing, such as analysis of traffic capacity, and investigating criminal business, management, library, etc. Since every job involves a large amount of data in each of these areas, when handling the related data application of cloud computing, the work efficiency and working process will be improved greatly, while the security and privacy of data involved in cloud computing is more important. Once the data involved is lost, the consequences as a result are huge and unimaginable. Thus it has very realistic significance to study and improve the network security technology in the cloud computing environment.

2. Advantages of cloud computing environment
Cloud computing, which is a new kind of calculation based on the Internet. In the way of cloud computing, hardware and software resources and information can be provided to a computer or other device in accordance with the need to achieve resource sharing. The distributed processing, cloud storage and virtualization technology greatly reduces the cost and the facilitation of the network life. Cloud computing generally has the following characteristics. Firstly, it has the data storage center with high security reliability. Secondly, cloud computing is convenient and fast and consumers can access the resources at any time, and use it whenever necessary. Thirdly, cloud computing has the characteristics of data sharing. It can provide a shared platform for data and applications between
different devices. Fourthly, it has unlimited scalability. Cloud computing provides unlimited possibilities for users of different numbers of different regions to use the network. In the context of cloud computing, the computer software hardware data that avoids accidents and stolen with human factors to ensure the integrity and security of computer network data information. Nevertheless, open to the Internet will decrease the security of computer network. Therefore, taking effective preventive measures to improve the security of computer network is necessary. Cloud computing has the safety and reliability because it not only provides users with accurate computing capacity, but also has a secure and reliable storage space. Therefore, users don't have to worry about data loss and viruses. Cloud computing uses interchangeable node isomorphism and data fault-tolerant measures to ensure the reliability and accuracy of "cloud". So compared with the local computer, use the "cloud" will be more safe and reliable. Cloud computing is a kind of economic use of the network technology. It won't go to for a particular application, but to create a variety of applications. Therefore, different applications may be in the same "cloud" with the support of running. Cloud computing can reduce the demand for investment in infrastructure, such as computers, and, in turn, reduce the cost of users. It can also effectively improve the performance of the computer, and reduce the expenses of software maintenance, etc. At the same time, the powerful storage space of cloud computing and the unimaginable computing power can effectively utilize and share the different resources between different devices, and reduce the cost of individual use creatively.

3. Network security risks in cloud computing environment

3.1. Network data communication risks
Cloud service provider on the cloud computing platform can take advantage of the software platform of efficiently to create a personalized and distinctive service system, which is the biggest difference between traditional information technology and cloud computing technology. Cloud computing service providers can provide the corresponding services according to user's professional interests, preferences, etc. Users can customize their information, so that it is helpful to reduce the information pollution, information garbage problem, which is of great significance to develop the healthy and harmonious society. But in the process of providing personalization information service, information leakage problems may arise. In order to their own interests, without the authorization of the user or the permission of user, individuals or enterprises collect monitor and spread some personal privacy information through the cloud computing technology. Some illegal molecules or cloud computing services in the profitable company may also use user access records on the client deliberately. They analyzed the web pages users browsed to study the cloud computing services user adopted in. They can also adopt cloud computing technology to collect, track much information such as personal relationship, family background and personal information and other relevant circumstances, which is a violation of user privacy and lead to unfair trade easily. It may also induce consumption deliberately and damage the interests of the users. Leaking user data privacy not only violates users' privacy, but also greatly increases the difficulty of the privacy protection of cloud computing's new service mode. For example, companies or cloud computing providers are not asking users for permission to collect and view users' stored data and information. Because of the characteristics of cloud computing technology, the ownership of the data information of the users is not only owned to people themselves, cloud computing service providers and other suppliers as well as the various countries government have the right to check the information data.

3.2. Network environment risks
Network environment itself is insufficient, which gives the chance to hackers to attack database system through the network. The confidentiality and integrity of database system are threatened. For example, loophole existing in the electronic mail makes the information storage security face much threat. In traditional network environment, data is shared in a single storage mode. Thus the security is mainly from a single computer's own security system. However, in a cloud computing environment, data is
stored in network operators cloud platform, allowing users to access it. The security in the process of using the network has become detector of integrity network operators. In addition, the network system also has the defects of the identity authentication, which makes the authentication become one of the main target hacker focuses on. The hackers thieve the information such as user information and password by invasion into cloud platform, or plant bugs in the platform through the cloud network environment, in order to steal the user information. In the public network environment, the sharing and transparency of data is more improved than that of single machine, and computer network security vulnerability is also one of the risk factors of computer system. As a public open environment, all information and data in the network are able to directly access to. If you are not pay attention to network security management in the computer system, the privacy information will be stolen. For example, if a computer system did not install a firewall, or did not set login user name and login password, or the login user name and password of the system will be easily to be intercepted by some website, making the computer system completely exposed to the public under the network environment.

3.3. Network protocol risks
There are two situations in network protocol. First is the vulnerability of the agreement itself. The second is the flaw in the protocol service. The attacker will attack vulnerabilities in several layers of the network such as the protocol's application layer, network layer, transport layer, and data link layer. In data link layer, each computer is on a network node. When they are sending packets on the same communication channel, the attacker can change the channel to send the error data packets to network nodes to replace the original packets in the process of sending packets. This behavior is to make appearances, which seems to be that there is no difference between the situations and the original situations. The packet will be hidden after a period of time, and then use the information in the system through the anonymous way, to spread the virus by email, or to steal the user name and password of web users. Sometimes attackers can damage the system through a firewall's vulnerability, which can cause a lot of damage to computer users.

4. The current common computer network attack method in cloud computing environment

4.1. Exploit vulnerabilities in network system
Due to the negligence of network management or the nature of the system, there are some loopholes in network system, such as UNIX, NT, Windows, etc. There are some holes in the system. Programmers are programmed to design programs that are unreasonable and unscrupulous about the logic of the program, resulting in one or more vulnerabilities that provide the population with the virus's invasion. The most typical flaw is the Chinese input method vulnerability of Microsoft Windows 2000 users. Non-authorized personnel can bypass Windows user name and password authentication with the help file of the login interface to get the highest permissions of the computer. There are also Winrar's self-decompression features, which are designed to facilitate the user's use, so that users who do not install Winrar software can also decompress files that are compressed in this way. But this function has been used by hackers for improper purposes. Take Universal plug-in and Play service vulnerability as example. Universal plug-in and Play allows an attacker to execute arbitrary instructions. There are serious holes in UPNP services the Windows operating system starts by default. UPNP system for wireless devices, PC and intelligent application, provide general peer-to-peer network connection, between household information equipment, office provide function of TCP/IP connection and Web access, the service can be used for the detection and integrated UPNP hardware. UPNP has vulnerabilities that allow an attacker to illegally obtain any XP system-level access. Network hackers exploit the vulnerability of network system to attack the system and steal the privacy data. In order to prevent the attack on the network system vulnerability, the network management should avoid human negligence and install the patch software to fix the system vulnerabilities timely.
4.2. Back door software attack
Attackers send an email or file, or induce the host operator to open or run an email or file with hidden Trojans. Then the trojan program will create a back door on the host. The other way is that an attacker attacks a host, gains control, and creates a back door on the host, in order to install a trojan program for the next intrusion. There is also a back door that was introduced in the software development process. In the software development phase, the programmers often create a defect in a back door to test or modify the program within the software. Then the back door was neglected by intentionally or unintentionally and not deleted when the software is released. Thus the back door exists inherently in the software.

4.3. Denial of Service attack
Denial of service attack is one of the most frequently used attacks by hackers to get the target machine to stop providing services. Actually the attrition of attack on network bandwidth is only a small part of the denial of service attack. If the attack can cause trouble to the target and make the system suspend or even crash, then the attack belongs to a denial of service attacks. The problem of denial of service attack has not been solved properly because of the security flaw in the network protocol itself. Thus the denial of service attack becomes the ultimate method of the attacker. An attacker makes a service attack to allow the server to achieve two effects effectively. First is to force the server to be full and not to accept new requests. The second is to use IP spoofing to force the server to reset the connection of illegal users to legitimate users. Another target of denial of service attacks may be to produce added costs for the application operator, when the latter uses resources based on cloud computing. In this case normally application used resources are tied to a needed Quality of Service level and this rule is usually linked to automated software to raise more virtual resources from the provider in order to meet the defined QoS levels for the increased requests. The main incentive behind such attacks may be to drive the application owner to raise the elasticity levels in order to handle the increased application traffic, in order to cause financial losses or force them to become less competitive. Other floods may use specific packet types or connection requests to saturate finite resources by, for example, occupying the maximum number of open connections or filling the victim's disk space with logs.

4.4. Malware injection attack
Malware injection attack uses malicious instance instead of system service instance to handle the normal service request, and to gain privileged access, certificate of illegal in order to steal information or user data. Different from traditional Web applications, virtualization features of cloud computing environment intensified security threat for malicious code injection attack. The cloud service migration, coexistence of virtual machine operations such as make malicious code detection work difficult, still lack of effective inspection method for cloud service instance integrity.

4.5. Cross VM side channels attack
Cross VM side channels attack is a kind of common forms of access drive attack. It requires the attacker and the target virtual machine to use the same physical hardware and execute interactively. In the process of execution, attackers can deduce the behavior of the target virtual machine, and to identify the server host information. The attacker firstly access to a shared hardware and cache with the help of a malicious virtual machine, and then perform predetermined security attacks, such as timing side-channel attacks, side-channel attacks of energy consumption. Attacks mentioned above are generally difficult to leave a mark or trigger alert. Thus it is impossible to avoid detection. Timing side channel attacks can obtain the information of users and servers by measuring the execution time of different computing tasks. Using the energy consumption log to launch attacks can help attackers quickly identify the type of target virtual machine hypervisor.
5. Network security protection technologies in cloud computing environment

5.1. Leak Scanning Technique
The technique is to automatically detect the local host or remote host security, to query the TCP/IP service port, to record the host response, and to collect relevant information in a particular project (Fig. 1). Application security scan is the realization way of the technology in a relatively short period of time. The scanner will be computer security vulnerabilities to find out, scan through the system after the completion of all output formats, easier for programmers to analysis and reference.

![Fig. 1 Leak Scanning Technique](image1.png)

5.2. Firewall Technology
The technology is used to strengthen the internet access control and avoid the external internet users into the internal network through illegal ways (Fig. 2). The internal operating environment can be protected effectively. All network information will be filtered through firewalls, and control access to the Internet information flow in accordance with the firewall security. The firewall itself is also stronger. A firewall can keep a hacker from entering a computer system to avoid the system being destroyed or computer data or information being copied.

![Fig. 2 Firewall Technology](image2.png)

5.3. Intel Execute Disable Bit
When the computer is invaded by the computer virus, the virus should be accurately judged by active defense technology, and the computer virus can be effectively intercepted. Antivirus software which is effective against virus is two kinds of software, Internet antivirus and single computer antivirus. The single antivirus software refers to virus scanning and thorough removal of computer remote resources by analyzing the scanning measures. Internet virus protection software pays more attention to network antivirus. If viruses were found in network or transmission network, network antivirus software can detect and wipe it out immediately. Thus the computer system should establish perfect anti-virus system to back up the regular data on computer systems and related documents in order to prevent the virus invasion of the operating system crash, data loss, in order to effectively reduce the loss brought by computer virus invasion. Moreover, the use of pirated software in computer systems must be used to
ensure that the network administrator gives the visitor permission to deny any unrestricted access within the scope of his work.

5.4. Network access control technology
The technology is to prevent unauthorized users to access to the system. Network access control technology is also carried out on the network security protection and the effective protection of a core strategy. Network access control technologies include access control, attributes control, internet access control, etc. The net access control can offer the first layer control area access control technology for internet access control mechanism, and users can access network resources by controlling the access site and access time of users.

5.5. Authorization access
There are many computer network security methods similar with firewall method, such as the data encryption method and the authorization access method. The data in computer network is encrypted, or the user is authorized to access control, making system easy to operate and easy to control, which can be widely used in open network. The data encryption processing technology in the current computer network is mainly controlled by the key and the encryption. The public key is widely used, such as RSA. Public key in encryption is an open and can be used and sent to the users of private key encryption under their own demand.

6. Conclusion
With the popularity of computer equipment and the rapid development of Internet technology, computer and Internet based applications have deep into the social from all walks of life, in every aspect, almost all industries, including power, construction, transport, police, finance, communication in the aid of computer and Internet technology to improve its information level of enterprise management and operation, improve the work efficiency of whole enterprise as well as the process standardization. The cloud computing environment refers to the integration of terminal devices, such as computers distributed on the Internet, to realize hardware and software resources by means of some kind of network calculation. The security of network of cloud computing environment faces many risks and threats. It is of great significance to take effective measures to avoid the attacks and increase the security.

References
[1] Cao Kehao. The study of path of network security technology based on cloud computing [J]. Network Security Technology & Application,2017,(09):94-95.
[2] Zhao Xin. The realization of network security technology based on cloud computing environment[J]. China New Telecommunications,2016,18(18):125.
[3] Yan Sheng, Shi Miao. The realization of network security technology based on cloud computing environment [J]. Computer optical disk software and applications,2014,17(23):168+170.
[4] Chen Yaru. Research on user behavior authentication and security control in cloud computing environment [D]. University of Science and Technology Beijing,2012.
[5] Li Chunlin. Research on distributed access control security policy [D]. Northwestern Polytechnical University,2005.
[6] Chen Huiyuan. Research and application of computer information system security technology [D]. China Academy of Railway Sciences,2004.