An Exploration of Cloud Security of the Hospitals with Internet Access

YUAN Junyi, LE Jiajin
DongHua University, Shanghai, China

***Abstract*:** Computing technology is the development direction of IT industry, and has become one of the most advanced technologies in various countries. At present, the bottleneck of cloud computing is cloud security. Cloud security is mainly reflected in the user data privacy protection and the traditional Internet, hardware, equipment security in these two areas. The traditional anti-virus mode is no longer suitable for the new network security situation. With the popularity of the Internet, various Trojan rampant, especially to profit for the purpose of the number of hacking Trojans soared. Trojan horse in all Internet security threats accounted for more than 90%, has replaced the virus has become the most important threat facing the internet. The proposed work is the general overview of the existing work that will be meaningful.

Keywords: *Hospitals, the Internet, cloud security, exploration, overview*

I. Introduction

Computing technology is the development direction of IT industry, and has become one of the most advanced technologies in various countries. At present, the bottleneck of cloud computing is cloud security. Cloud security is mainly reflected in the user data privacy protection and the traditional Internet, hardware, equipment security in these two areas. To achieve cloud security, you have to solve several problems. Finally, point out the specific use of cloud security technology to solve cloud security issues, and attached to the cloud security investigation report.

Cloud computing is currently the most popular topic, Google, Microsoft, IBM, and SUN have released cloud computing plans and related products. Through the network will be huge computing program automatically split into numerous smaller subroutines, by searching, calculating, make huge system composed of many servers after the analysis results will be sent back to the user. Through this technology, network service providers can reach tens of millions or even billions of information in a matter of seconds to achieve the same powerful network services as supercomputers.

Cloud computing this calculation model is applied to the field of information security, so as to produce a new anti-virus concept called cloud security, cloud security is the concept of enterprise creation, become an independent school in the international cloud computing. It will anti-virus software in the past passive, anti-virus upgrade to take the initiative to detect web security risks, thereby actively blocking malicious network code, in order to protect the network and personal computer security.

According to the monitoring data of rising company and other domestic companies, the number of computer viruses has increased explosively in recent years, and has spread quickly and has a wide range of hazards. More than 20 thousand new virus programs are present every day. Now, the virus's production speed almost reached the limit of security vendors' detection and analysis capabilities. The emergence of new viruses and the growing feature library of viruses have greatly increased the difficulty of security vendors in capturing and processing virus samples. Traditional anti-virus software mainly through the characteristics of the code compared to intercept and kill viruses, the relevant data show that each security vendor can only capture about 10% of the new virus every day. The traditional anti-virus mode is no longer suitable for the new network security situation. With the popularity of the Internet, various Trojan rampant, especially to profit for the purpose of the number of hacking Trojans soared. Trojan horse in all Internet security threats accounted for more than 90%, has replaced the virus has become the most important threat facing the internet. Trojan is often hidden in the user's computer system, forcing pop-up advertising, recording keyboard information, illegal access to user files, stealing online banking, online accounts. To profit for the purpose of Trojan horse, according to customer demand, customization, development and other characteristics, Trojan behind the formation of a huge black industry chain. According to reports, the horse industry chain has developed very perfect, and Trojan production, communication, control, free to kill the packers, broiler hacking, fence the division is quite clear, forming a perfect line and the growth rate is very alarming. The commercial hacker group with Trojan horse as the main tool poses a great threat to the Internet economy.

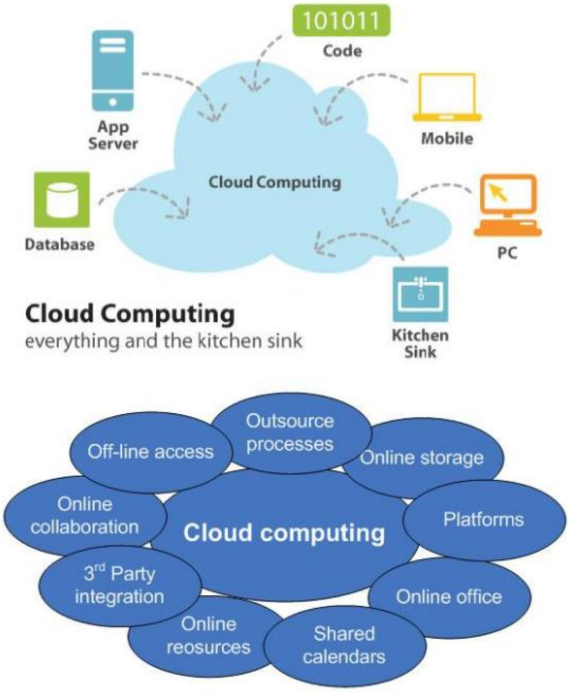

Fig. 1. The Cloud Computing Paradigm and Model

II. The Proposed Methodlogy

Definition of cloud computing. Cloud computing is the development of distributed processing, parallel processing and grid computing, or the commercial realization of these computer science concepts. It is a super computing model based on internet. It uses the transmission capacity of high-speed Internet to deal with data from a personal computer or server to a super computer cluster on the Internet, the computer server group is the industry standard by tens of thousands of Taiwan is very common, by a large data processing center management. Cloud computing is a virtual pool of computing resources, which provides users with computing resources in the resource pool via the internet. Complete cloud computing is a dynamic computing system that provides managed application environments that dynamically deploy, dynamically distribute computing resources, and monitor the use of resources in real time. Cloud computing, the emerging method of sharing infrastructure, is facing an ultra large scale distributed environment, the core is to provide data storage, data processing and network services. In fact, the simplest and most original cloud computing is already ubiquitous on the Internet, such as search engines, web mailboxes, and so on.

Definition and development of cloud security technology. In the field of network security, the traditional methods for the discovery of the virus antivirus, anti virus samples analysis by the engineer of the Virus Inc, and then according to the samples of the virus code uploaded to the virus database, the user through the timing or manually update the virus database, to get upgrade anti-virus protection software.

But in this way, the virus code updates more troublesome, users upgrade antivirus software every day, it also consumes memory and bandwidth. Build a powerful cloud around the world through the server, the virus code in the cloud is completely able to intercept the virus, and it also greatly reduce the client's processing task, reduce client memory, without time anti-virus and upgrade software. Because clouds and clients interact with each other through the Internet at any time, all calculations are carried out on the cloud, which saves costs and time, effectively controlling the spread of the virus. This is the "cloud security", it combines the parallel processing and grid computing, the behavior of unknown viruses other emerging technologies and concepts to determine, through in the network monitoring software abnormal behavior in a large network of clients, get the latest information on the Internet, malicious Trojan program, sent to the Server side for automatic analysis and processing, then viruses and Trojans solutions distributed to each client. The whole Internet is a huge "antivirus software", the more participants, the more secure each participant, the entire Internet will be more secure.

Internationally renowned security vendors, trends, technology and domestic rising has played a "cloud security" slogan, which for users, is undoubtedly a huge positive. Of course, not only is the anti-virus vendors, international well-known security vendor Web Web-sense, in the aspect of malicious code collection and emergency response also make full use of the characteristics of cloud computing, with its deployment in the global scope of grid computing, can timely response to network attacks appear constantly new, provide strong support to update the virus database. Moreover, the application of cloud computing in the security field greatly promotes the changes in the traditional security industry, and perhaps in the near future, security vendors will follow the trend, and truly realize the "software as a service" marketing model.

Cloud security policy. In view of the current grim security situation in the Internet, in order to fully respond to the challenges of the Internet security situation, domestic security vendors quickly introduced a security system that focuses on the entire Internet Defense, that is, cloud security. Cloud security is the latest manifestation of network security in the Internet era, cloud security is derived from the concept of cloud computing, cloud computing, P2P technology, parallel processing technology hybrid development, the natural evolution of the results. By a large number of client (client) abnormal monitoring of software and software behavior, collect and summary of the latest malware, spam or phishing websites, get the latest information on viruses and other malicious programs in the internet. Once an exception is detected, it is submitted to the cloud (server group) for automated analysis and processing in a timely manner, and the solution is fed back to each client. The entire Internet is a huge malicious threat fast passive response system, it will be a large number of users to integrate organically, sharing all voluntary users to join security threats submitted information. The more users involved, the safer each participant will be, the more secure the entire Internet will be. This is a major breakthrough in anti-virus software, which can respond quickly to new threats, greatly reducing the pressure on the client and maximizing the power of the public.

The core of cloud security is to detect and identify the entire network risks and threats at the fastest possible speed and give early control. In recent years, memory consuming feature files have grown exponentially. Cloud security keeps most of the feature files in the cloud, while keeping the minimum number on the client side. This approach reduces bandwidth consumption and provides faster and more comprehensive protection in time. The core of the cloud security program is to allow users to participate in the prevention and killing process. Because a large number of virus samples are acquired through the client, that can be changed from antivirus to antivirus.

Cloud security is also a good way to deal with growing spam. Spam sends the same content to millions of receivers. Spam can be filtered and dealt with by collaborative computing on a large scale of users. The working principle: the client first for each message received can only calculate the mark recognition, the number of copies of the same message statistics by comparing the mark, when the copy number reaches a specified number, you can determine the mail is spam. Each user who joins the system is not only the object to receive the service, but also a terminal to realize the distribution statistics. This large-scale statistical method of filtering spam is not prone to miscarriage of justice, and practical. Use a large number of clients to work together to build a spam firewall.

Limitations of Cloud Security. The more clients, the more secure each user is, because a large group of users is enough to cover every corner of the Internet, and as soon as new threats emerge, they are immediately detected and intercepted. But to build cloud security, and to achieve normal operation, is not easy. First of all, the need for massive client and broad user market distribution. The more clients there are, the more sensitive it is to the identification and detection of various threats on the internet. No matter which client encounters a threat, it can respond at the first time and submit it to the cloud for analysis and processing, and then feed-back the threat solution to each client.

Secondly, strong core technology and rich experience in anti-virus cannot be separated. Network threats are detected, should be analyzed at the first time, which requires excellent technology, otherwise it cannot achieve the fast response of cloud security.

We need to put in a lot of manpower, money and equipment. Cloud security requires security vendors have a strong technical team and ongoing research, while the server, bandwidth and other aspects of the need for a lot of money invested. Cloud security is based on cloud database and cloud computing, security program programming is very different, and the establishment of cloud database also requires security vendors have a certain size and financial strength. The key to the implementation of cloud computing is how to decompose a task effectively and assign sub tasks to parallel servers in different regions. To truly play the role of cloud computing, not only need the corresponding professional software support, but also need a strong mass of data processing capabilities.

Cloud security should be an open system that allows other security vendors to join and be compatible with cloud security. For ordinary users even if users use different anti-virus software or different security vendors can share cloud security, cloud security and safety results, it can realize the true meaning of the participants more security "on cloud security. In practice, however, these are not easy to implement.

Finally, user privacy is always a very important issue that security vendors cannot avoid, and cloud security contains risks related to user privacy. Security vendors define the extent to which users' secrets can be detected and collected in a user agreement. If unilateral determination appears to be contrary to fairness, legislation is needed to regulate it. To adapt to the arrival of the era of cloud security, the existing legal system will have a process of adjustment, there are still many problems we need to solve.

CONCLUSION

Cloud security shifts the computing power of the original client to the cloud, thereby reducing the pressure on the client. There is no denying that cloud security is the future direction of network security. Cloud security can maximize the release of user computer system resources, for users, do not frequently upgrade the virus library and feature code, and security protection is more comprehensive, fast and perfect. More important is to subvert the traditional post virus feature code defense model. With the rapid development of the Internet, new threats are always emerging. Although the debate about cloud computing is mixed, the hospital must guarantee the security of the information to the users. In the development of computer network technology more and more time, we must pay attention to personal information security and data security issues, strengthen security and defense technology research, the daily work and life network technology to better serve the people.

References

[1] Almorsy, Mohamed, John Grundy, and Ingo Müller. "An analysis of the cloud computing security problem." arXiv preprint arXiv:1609.01107 (2016).

[2] Ryan, Mark D. "Cloud computing security: The scientific challenge, and a survey of solutions." Journal of Systems and Software 86.9 (2013): 2263-2268.

[3] Shahzad, Farrukh. "State-of-the-art survey on cloud computing security Challenges, approaches and solutions." Procedia Computer Science 37 (2014): 357-362.

[4] Pantangi, Ajay, Kaiqi Xiong, and Mufaddal Makati. "SECUPerf: End-to-End Security and Performance Assessment of Cloud Services." Trustcom/BigDataSE/I SPA, 2016 IEEE. IEEE, 2016.

[5] Duncan, Bob, and Mark Whittington. "Enhancing Cloud Security and Privacy: The Cloud Audit Problem." Cloud Computing (2016): 119-124.

[6] Afolaranmi, Samuel Olaiya, et al. "Methodology to obtain the security controls in multi-cloud applications." (2016).

[7] Jung, Christian, Andreas Eitel, and Reinhard Schwarz. "Enhancing Cloud Security with Context-aware Usage Control Policies." GI-Jahrestagung. 2014.

[8] Tang, Changlong, and Jiqiang Liu. "Selecting a trusted cloud service provider for your SaaS program." Computers & Security 50 (2015): 60-73.

[9] Mallareddy, A., V. Bhargavi, and K. Deepika Rani. "A Single to Multi-Cloud Security based on Secret Sharing Algorithm." International Journal of Research 1.7 (2014): 910-915.

[10] Avram, Maricela-Georgiana. "Advantages and challenges of adopting cloud computing from an enterprise perspective." Procedia Technology 12 (2014): 529-534.

[11] Balamurugan, B., and P. Venkata Krishna. "An Enhanced Security Framework for a Cloud Application." Artificial Intelligence and Evolutionary Algorithms in Engineering Systems. Springer India, 2015. 825-836.

[12] Singh, Jitendra. "Comprehensive solution to mitigate the cyber-attacks in cloud computing." International Journal of Cyber-Security and Digital Forensics (IJCSDF) 3.2 (2014): 84-92.

[13] Irimie, Bogdan-Constantin, and Dana Petcu. "Scalable and fault tolerant monitoring of security parameters in the cloud." Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), 2015 17th International Symposium on. IEEE, 2015.