Journal of Applied Science and Engineering Innovation, Vol.5, No.3, 2018, pp. 65-68
ISSN (Print): 2331-9062
ISSN (Online): 2331-9070

Information Resources Sharing Security in Cloud Computing

Ran Li[1], Rui-feng Yu[1], Xiao-shuang Wang[1]
[1]*College of Information and Communications, National University of Defense Technology, Xi'an, Shaanxi, 710106, China*

Abstract: With the wide application of cloud computing, cloud computing security issues are now becoming more and more popular. By analyzing the security of information resources sharing in cloud computing environment, this paper discusses the technical, political and social issues of security protection.

Keywords Wireless Networking, Security Technology, cloud computing

INTRODUCTION

With the development of cloud computing, security issues have become increasingly prominent, becoming an important factor restricting the development of cloud computing[Garfinkel, et. al., 2010]. More and more companies hold a skeptical attitude towards cloud computing because of security issues. According to IDC reports, there are more than 74% of users believe that security issues are the main problem limiting the development of cloud computing[Li W, et. al., 2010].

Network information resources refer to all the electronic information resources put into the Internet collectively, playing a very important role in the information age[Kantarcioglu, et. al., 2004]. It brings about full information values to us, however, at the same time, also produces a series of problems, such as false information released in network resources, confidential information leakage caused by hacker attack and so on[D. He, et. al., 2013]. Therefore, how to solve the security issues in network information resources is increasingly important.

THE ISSUE OF INFORMATION RESOURCES SHARING SECURITY IN CLOUD COMPUTING

The Gartner company in US believes that cloud computing is mainly confronted with the following seven security issues:

Risks of privileged user access. Privileged user management data is likely to bypass the regulation of internal procedures for control, thereby causing security risks to sensitive data from the outside of the enterprise[Feng Min, et. al., 2006];

Compliance risks. Due to the data is submitted to the service provider for supervision, if it refuses to accept supervision and audit, it is the customers themselves who must be responsible for the security and integrity of the data;

Uncertain data storage location. Because of the virtualization technology and distributed storage, the location of managed data in unclear. And cloud providers may also pose a threat to the data security;

Data separation risks. Given that multi-users' data is stored in a shared cloud environment, precise data isolation should be assured[Rajkumar, et. al., 2009]. Encryption is an effective method, but it is likely to have an impact on the availability of the data;

Data recovery. When a disaster occurs, whether the provider of the data and services will recover the data also affects the security of the data;

Survey support risk. Because the users' log files and data may be stored together, also may be scattered in a constantly changing host and data center, so is unlikely to legally investigate the cloud computing environment;

Risk of long-term availability. When the service provider is acquired, it is also important to ensure that the restored data is still available[Mell P, et. al., 2009].

INFORMATION SECURITY MEASURES IN CLOUD COMPUTING ENVIRONMENT

Cloud computing security is to provide services to users in the open and complex cloud computing platform, and to ensure the security and reliability of user information[S. Chen, et. al., 2010]. Cloud computing security issues should be carried out from many aspects, especially the technical level. As shown in Figure 1, it is a security model of cloud computing technology.

PREVENTION AND SOLUTION FROM A TECHNICAL POINT OF VIEW

Physical security

Physical security is to protect the computer network equipment, facilities and other media from earthquakes, floods, fires and other environmental accidents and artificial operation errors and a variety of destroy caused by computer crime. It mainly includes 5 aspects: environmental safety, equipment safety, media safety. To ensure the physical security

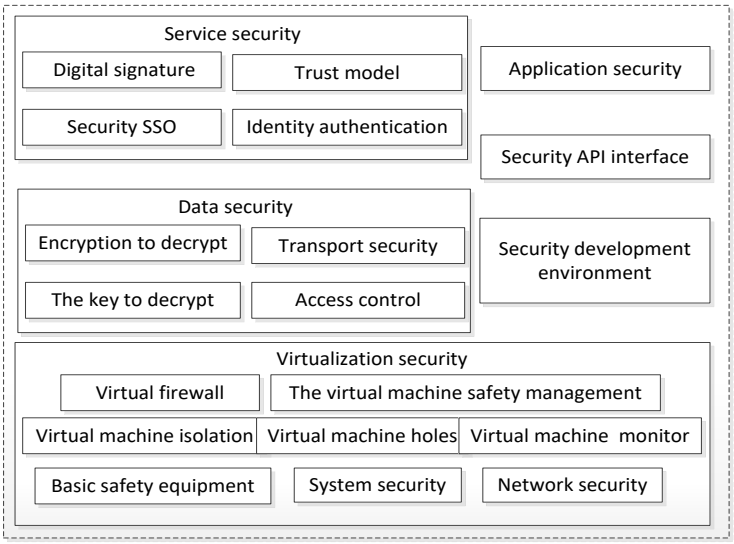

Figure 1 The security model of cloud computing technology

of computer information system is the premise of the whole computer information system security.

Access controlling technology

With the help of improved access controlling technology, a firewall (including packet filtering and application proxy) is set up between the internal network and external network, which have already been isolated, to prevent the external network users access the internal network resources illegally and protect the special network interconnection devices in the internal network environment. It implements the inspection on the transmission of data packet between two or more networks, to determine if communication between the networks is allowed, monitor the running state of the network and achieve internal and external network isolation. At the same time, access control is achieved with the "write upward and read downward" mandatory access control technology to protect the safety of internal network, which is one of the most important and the most effective and the most economic measures[Xie, 2012].

Cryptography

Cryptography is one of the most important methods in protecting information security. It is a combination of mathematics, computer science, electronics and communication of many sciences in a body of interdisciplinary[Y.Ma et. al., 2012] It not only has to ensure confidentiality of information encryption function,

but also has a digital signature, authentication and secret saving, system security function and so on. Therefore, not only the confidentiality of information, but also the integrity and authenticity of information can be guaranteed to prevent cryptography and asymmetric key cryptography. There is also a public key system proposed by W.Diffie and M.Hellman.

Virtual private network technology

Virtual Private Network (VPN) is a technology developed rapidly in recent years with the development of the Internet. More and more modern enterprises use the Internet resources to promote sales, sales, after-sales service, and even training, cooperation and other activities. Many companies tend to use the Internet to replace their private data networks. The logic network which uses the Internet to transmit private information is called virtual private network. At present, VPN mainly uses four technologies to ensure the security, these four technologies are tunnel technology, encryption and decryption technology, key management technology, and authentication technology.

Safety isolation technology

Network security threats and risks are mainly in three aspects: the physical layer, protocol layer and application layer. Maliciously cut off or communication interruption caused by high voltage belong to physical layer threat; fake network address, teardrop fragmentation attacks, SYN Flood, belong to the protocol layer threat; Illegal URL, malicious page codes, mail virus belong to the application layer attacks. From the point of view of security risks, attacks from the physical layer are rare, attacks from network layer are often, while attacks from application layer are common, which are difficult to prevent because the complexity and diversity. In the face of the constant emergence of new network attacks and the special needs of high security network, the new security concept "security isolation technology" was brought up. Under the premise of ensuring that the harmful attacks are isolated from the

trusted network and that the internal information of the trusted network is not compromised, its goal is to exchange information among networks safely.

SSL protocol and SET protocol

These two protocols are mainly used in the process of e-payment. SSL protocol (secure sockets layer protocol) can improve the security of data transmission between applications. Therefore, it is mainly to provide the authentication between the user and the server. The transmission security is ensured by encrypting the data. ETS protocol, the secure electronic transaction protocol, is a protocol based on information flow, which is used to ensure the security of the bank card payment transaction on the public network. It is a trusted third party certification center which reflects the various relationships of the parties to the card transaction.

Security audit

In a cloud computing environment, both the user's data and computation are out of control. Therefore, it is necessary to audit the behavior of users and providers, to ensure the correct implementation of security policies, and to maintain the organization compliance. Literature Ryan KL Ko et al. proposed Trust Cloud framework, based on the method and technology to solve the problem of security audit in cloud computing environment. Audit Cloud project aims to provide basic support for ensuring the credibility and transparency of private and public cloud. Chen and Wang et al. studied on the auditing of the cloud computing, and put forward a CSIRO prototype system, which is an audit of the services deployed in the cloud computing environment.

PREVENTION AND SOLUTION FROM THE PERSPECTIVE OF POLICY AND REGULATION

It is very necessary to formulate the norms of network information policy and law to regulate people's behavior on the network, so that Internet users can avoid security threats and solve security problems in the acquisition of online information resources. For example, develop intellectual property laws and regulations to solve the increasingly serious problem of network intellectual property rights, develop e-commerce law to improve the electronic commerce. Today, it is profoundly recognized that problems like commercial law, security and authentication, privacy, knowledge property protection, tariffs and taxes, electronic payment methods, management of Internet content, dispute solving mechanism and consumer protection laws have become the key to the development of electronic commerce.

PREVENTION AND SOLUTION FROM THE HUMANISTIC POINT OF VIEW

In the real society, we make all kinds of laws and policies to protect the social order, at the same time we pay more attention to the importance of social ethics to the social order. Also with the great development of the network, to maintain order in the social network, the "network morality" is also very important. It can promote the strengthening of people's awareness of network security, which is complementary with our laws and policies. The world is strengthening the education of information culture, which of course includes the importance of security issues.

CONCLUSION

The goal of building a complete security protection system is to reduce the unit network risk to an acceptable level. Network information security is a dynamic concept, there is no absolute security. In order to improve the unit network information security, it is very important to manage the network information, in addition to the use of adaptable, highly reliable security measures and products. Network information security is 30 percent dependent on technology while 70 percent on management. The negative impact brought by the negative impact is certain to decrease by effective network information management.

REFERENCES

D. He, C. Chen, S. Chan, and J. Bu. Di-Code: DoS-resistant and distributed code dissemination in wireless sensor networks. IEEE Communications Magazine, Feb. 2013.

Feng Min. Wireless network key security technology fusion research. Shandong Communication Technology, 2006 (02).

Garfinkel T,Matthews J,Hoff C,et al. Virtual machine contracts for datacenter and cloud computing environments[C] .Proceedings of the 1st Workshop on Michael Armbrust,ArmandoFox,Rean Griffithet.al. A View of Cloud Comput-ing[J]. Communications of the ACM,2010:50-58.

Kantarcioglu M, Clifton C. Privacy-preserving Distributed Miningof Association Rules on Horizontally Partitioned Data, Proc. ofIEEE Transactions on Knowledge and Data Engineering,2004-09:1026-1037

Li, W. Lou, and K. Ren. Data security and privacy in wireless body area networks. Communications, 17(1):51-58, 2010.

Mell P，Grance T. The NIST Definition of Cloud Computing[R]. National Institute of Standards and Technology，Information Technology Laboratory, 2009.

Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal etal . Cloud Computing and Emerging IT Platforms: Vision,

Hype, and Reality for Delivering Comput ing as the 5th Ut ility [J] . Future Generat ion Computer Systems, 2009, 25 (6) : 599- 616.

S. Chen and C. Wang, Accountability as a Service for the Cloud: From Concept to Implementation with BPEL[C]. Proc. 6th IEEE World Congress on Services(SERVICES-1),IEEE, 2010. 91-98.

Xie Jingxian, Innovation and development of 4G communication technology. Information Communication, 2012(4):207-208.

Y.Ma, T. Houghton, A. Cruden and D. Infield. Modeling the Benefits of Vehicle to Grid Technology to a Power System. IEEE Transactions on Power Systems, 27(2):1012-1020, 2012.