ISSN : 0974 - 7435 Volume 10 Issue 20

2014

BioTechnology

An Indian Journal

FULL PAPER

BTAIJ, 10(20), 2014 [12489-12496]

Research of building enterprise network security system based on cloud computing technology

Linjun Kong
Office of information technology, Zhejiang University of Finance and Economics, Hangzhou Zhejiang, 310018, (CHINA)

ABSTRACT

Network security is a problem needing us to pay more attention in this information age. No matter by enterprise or by individual person, cloud computing technology is widely applied to remain network security. This paper introduces a security management model based on cloud computing technology, which can deal with mass security events according to the large data provided by cloud computing. This model not only has overcome the deficiency of low efficiency but also has gained great improvement in data processing, so it has gained guarantee in security and reliability. Through dividing the network areas safely based on clouding technology, this paper has successfully built a series of real-time warning assets risk models, which can help managers manage the network security, and analyze abnormal events and risks. This security system is constituted of several subsystems responsible for early warning management and emergency response. Cloud security management system is divided into five hierarchies from high to low: user interface, cloud service layer, data processing center, the data collection layer and network security equipment layer. Through the united management by cloud computing platform, the model also can process some security events, efficiently lowering the possibility of existing network risks. The security management system based on cloud computing technology successfully improve the existing management system, expand its functions and promote the enterprise computer management.

KEYWORDS

Cloud computing technology; Network security; Management system.

© Trade Science Inc.

INTRODUCTION

The coming of information age has promoted the rapid development of computers and network technology, but accompanying with promoting enterprise's growth, the development of computer technology also has some drawbacks. The improvement of computer's performance is walking into the bottleneck period. The rapid development of network technology make it possible to share information and data all around the world, so in the computer age the efficient use of network data has gained more and more important meaning. Sharing network resources is a two-edges sword. The large repository can provide mass theoretical knowledge for people's life and production, but these resources can also be sued by lawbreakers to threat other's life or property. Network security problem has long been a difficult problem in computer technology development. Some lawbreakers make use of vulnerabilities existing in the security management system to steal the business information, greatly damaging enterprise's benefits. So it urgently needs a security management platform to safeguard the network security.

Security management platform is also called security operation center, which is a kind of network security management technology becoming popular in recent years. SOC is a management system normally used in nowadays. It can do simple analysis of data and take certain response measurements to some security events, but because traditional SOC's performance usually has a low security, once there are some breakdowns existing in SOC's relational engines, SOC would be gum up, making a greatly damaging effect on enterprise' s management. The application of cloud computing technology improves the defects of traditional SOC system, not only providing mass dynamic data but also greatly improving the data processing capability. So the improved SOC can resolve bugs in time, reducing the negative effects on the enterprise. Here, this paper introduces the building of enterprise network security system model based on cloud computing technology and studies the prosperity of cloud computing technology's application and development.

THE INTRODUCTION OF CLOUD TECHNOLOGY

The definition of cloud computing technology

Cloud computing technology has different definitions under different using situations. In network security management system, cloud computing is defined as a confluent product, involving grid computing, parallel computing, distributed computing and virtualization technology. Mass virtual repositories are organized through network sharing, whose virtual recourses are usually applied and managed by enterprises, and also can meet users' needs by providing computing service, data storage and platform service. Compared with other computing technology, cloud computing technology enjoys more advantages, such as supporting resource virtualization, great capability of processing and analyzing data, high scalability, high viability and more transparent service.

The features of cloud computing platform

From Figure 1 we can see that by shielding the details of implementing underlying soft and hard wares, cloud computing platform successfully reduce big data process loan, covenanting the system management. The special design of service interface enable every user to enter cloud computing platform to gain sharing resources. Now day's cloud computing platform is basically based on the basic technology framework of cloud computing. But because different companies and organizations have different security management systems. But the normal security systems can be divided into three categories: integrating basic resources to provide a computing platform for network service; the platform providing underlying basic resources based on virtualization technology; the platform providing best service resources with functional specialization and with a capacity of integrating internal resources provided in the platform. The basic technology framework of cloud computing platform is shown as Figure 1.

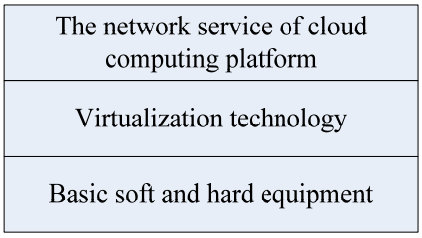

Figure 1 : Basic technology framework of cloud computing platform

But all cloud computing platforms, whatever kind it is and whatever aim it has, have three common features:

(1) Users can enter cloud computing platform through relative entrance without need to care the realization of cloud computing underlying platform.

(2) The usage of cloud computing platform is very flexible. Users can adjust the system according to the practical situation, improving its convenience and efficiency. Cloud can make use of network virtualization technology to service users, not only meeting users' need but also reducing cloud cost.

(3) The building of cloud computing platform is based on mass data or network data, so cloud platform can provide an efficient computing service. And because it has a great capacity of efficiently processing and analyzing data, so for its users resources provided by the cloud platform is unlimited and can meet users' various needs.

Cloud computing users' relations

According to Figure 2 we can conclude that in cloud computing because users are different so there are differences existing in supply-demand relations. Different users play different roles in cloud computing platform.

(1) The bottom of the relation is the cloud supplier, which are responsible for the basic operation of cloud computing and providing basic cloud equipment and service. To guarantee the normal operation of cloud platform is a relative big project, which needs to be contributed many equipment and human power, so it is usually the big company that is responsible for the project, because small company's human and financial resources unable to undertake such a complex and difficult project. One of excellent cloud suppliers is Amazon, which not only can provide the basic equipment such as ES2 but also cloud platform database. And all users can directly use and participate in these services. But cloud suppliers always provide basic cloud service, so their resolutions are usually simple and cannot provide users some special services. In order to fully meet users' need, the suppliers and users should make use of cloud computing platform to develop custom service.

(2) The middle users are responsible for developing service for specific target users and integrating cloud platform' basic application. The middle users can be divided into two group of users: one is service suppliers and the other one is direct users. They can be cloud's end users, a group of users who can directly use cloud service or make use of cloud platform to do their service to gain their own business profit through the second development of cloud platform. By this way they can develop software to gain economic benefit according to users' need. The middle users can rent resources provided by cloud platform, and then package and upgrade them. All the upgraded sources would be sale to the end users, by this way the middle users can gain economic benefits. In today's cloud platform service, most middle users choose the 3rd part application to gain benefit. This model is same as the popular TaoBao. Cloud computing platform provide a exchange platform for the middle users just like operating a shop in TaoBao, to make money by making business with end users. It will be more and more popular in the future to provide such service in cloud platform. And more serving software will be introduced to users. The adventures the middle users enjoy are that they can integrate specific service according to different users' needs, so their service would be all appropriate users. And the suppliers of cloud platform service can successfully cut their costs under the support of cloud platform's bottom service, much more than traditional IT service providers.

(3)The top users of cloud is end users, who use cloud platform according to service provided by cloud serving providers. They can receive services that meet their demand when they pay expenses. The supple-demand relation between cloud computing users and their hierarchy is shown as Figure 2.

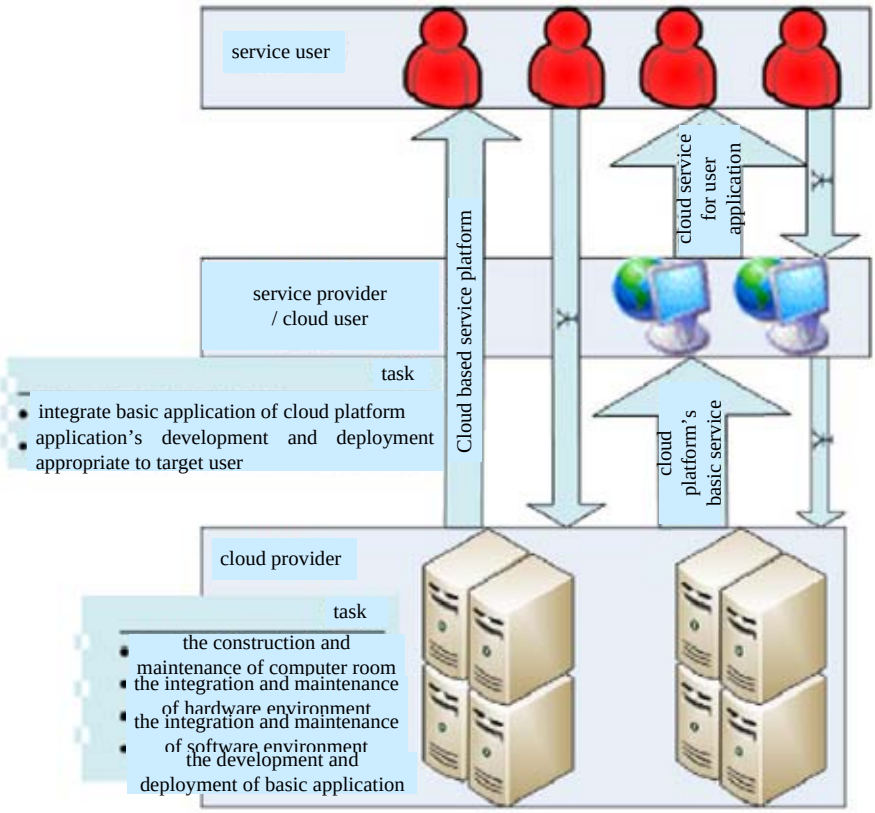

Figure 2 : The supple-demand relation between cloud computing users and their hierarchy

THE INTRODUCTION OF NETWORK SECURITY

The definition of network security

Network security points to the protection of hardware, data, information and software, aiming to avoid the faults and information leakage and loss due to spiteful attack. The serious accidents can make the whole network paralyzed and unable to operate or be used normally.

The essence of network security is to guarantee the transmission, sharing and safe usage of network information. The network security research includes information's integrity, authenticity, security and availability. The task to protect network security needs to comprehensively apply different kinds of technologies, including computer science and technology, information security management technology, mathematics and physics and telecommunication technology. Network is a comprehensive subject integrated in many kinds of technologies.

Network security technology

The management technology applied in network security

With the developing of network, market economy has been more closely integrated with network and network security also have gained more and more attention. The application of network security management technology by enterprise can make enterprise's management easier and win more benefits for enterprise. Once a company's network security faces great threat the company would suffer a great economic damage, making a negative effect on the company. So the development of network security technology cannot wait any more. There are some aspects need us pay more attention when it comes to network security management, such as equipment configuration and coordination, network security early-warning and network security risk monitoring. Network security management is an important part of the enterprise management system. Because in nowadays most companies' daily operation cannot be without network, so network security management concerns company's information and economic data, which once are leaked the company would suffer an unavailable damage.

Firewall technology

Firewall technology is well known by the public, because its name usually appear in mobile phone and computer. Network is a big information sharing platform and enterprise's network security management is like a small network, which needs firewall to protect it from threads from outside world. Firewall is a kind of protect system, which can do certain activities in the network and also the data exchange, protecting the whole network not be attacked. And through making use of cloud technology to setting firewall, the enterprise can freely transfer its data without being afraid of the outside interference. So enterprise can use firewall to isolate the information exchange between different network areas. The firewall, as an intersection of different local area networks, it can control the transmission of data based on the different setting conditions. Firewall not only can ensure the safe data transmission but also the safe information exchange, so it cannot be simply described as a kind of restriction system but a separation system and a analyzing system. Through efficiently analyzing data and exchanging data with the outside world firewall can successfully protect the whole network.

The reason why firewall is widely applied in the network security management system by the enterprise is that there is potential safety hazard existing in it, making information in the database more easily be leaked or steeled. Because the internet protocol settings doesn't fully considerate security factors, so it's necessary for the enterprise to apply firewall technology into the network security management system.

Intrusion detection technology

Intrusion detection technology is designed to protect database from the outside damage, which can detect abnormal activities that violates safety rules and threads the system's security. The network security management system can setting up the activities damaging the network, and intrusion detection technology can do risk assessment for users' activity or the system's activity. And it would notice the managers to resolve the damaging activities. Intrusion detection is mainly designed to do system detect, activity detect and distributed immune detection, which all play an important role in the enterprise's network security management.

THE INTRODUCTION OF APPLYING CLOUD TECHNOLOGY TO THE ENTERPRISE'S SECURITY MANAGEMENT SYSTEM

The Figure 3 shows us the building of the cloud security management platform model, in which asset is the core of the whole platform. The security events management, as the main process of system operation, makes use of cloud technology to classify the network area according to the safety condition, and then build a real-time asset risk early-warning model, which would help managers to manage the network and analyze the anomalous events and risks. The early-warning system and emergence response compose of a comprehensive security management system. The cloud security management system, from high to low, can be divided into five hierarchies, including user interface, cloud service, data processing center, data acquisition and network security equipment. The highest hierarchy is the service users and the lower one is the service provider.

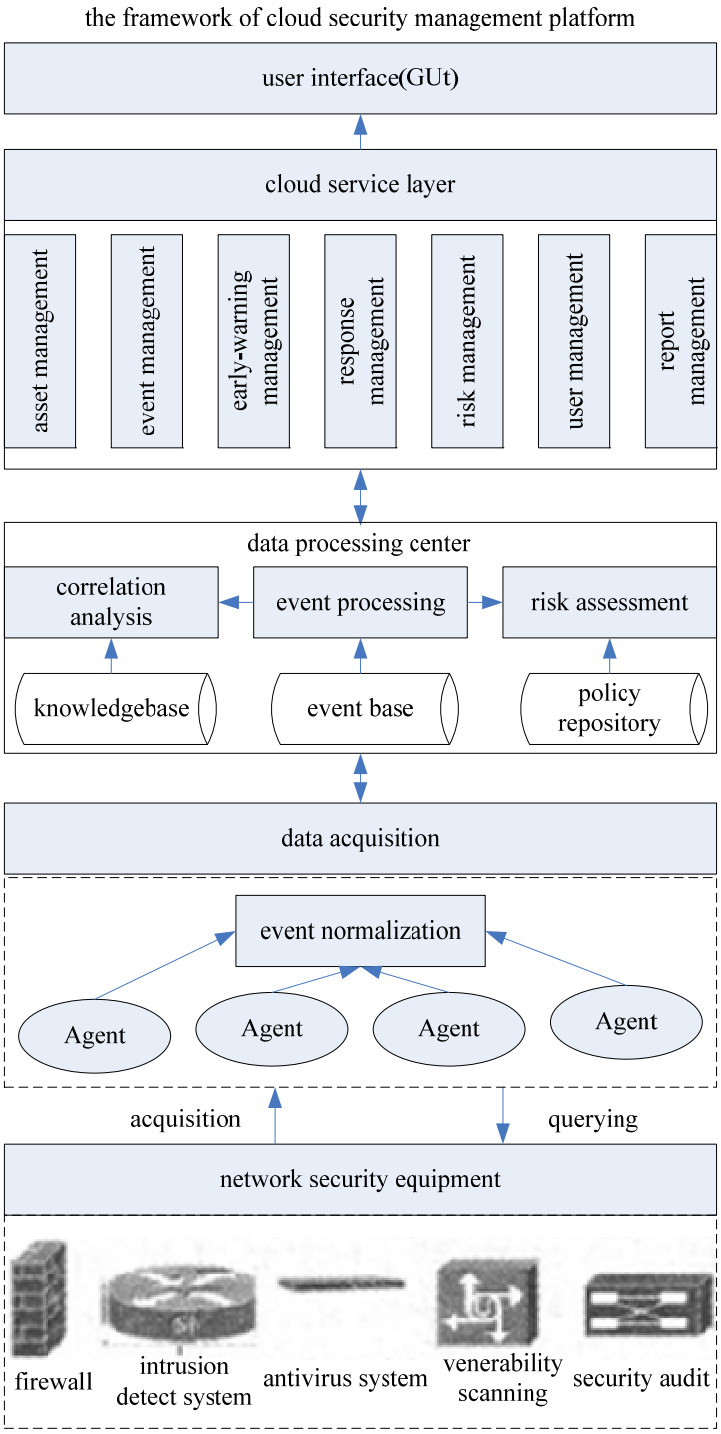

Figure 3 : The framework of cloud security management platform

User interface

User interface is the most important part of cloud management platform because the building of the platform is designed to provide service for users, this is also what the cloud platform managers should consider no matter what they do. User interface can provide users a visual management interface. Because of the application of the B/S model, users can directly enter the network and manage the network security equipment through the browser without the need to set up client software. And the users can also deal with the anomalous events according to the feedback information provided by the system.

Cloud service layer

Cloud service layer cooperates with user interface and it directly provides enterpriser service, including the following six services:.

Event processing

Enterprise can inquire the recent condition of the network system, design the events and manage them after doing audit. Such a service enable enterprise directly to find the abnormal condition of the network system and then rapidly take certain measures.

Risk management

Risk management is to do risk assessment for network security system. Users can gain network system's asset value through risk management. According to host computer or network's asset value, users can have a priority to upgrade the abnormal event and do the reliability analysis. If the assessment result is higher than the value specified by the system, the system would send warning sound.

Asset management

Asset is very important for the enterprise. Asset management is to manage the asset in the enterprise's network by monitoring the asset condition in time. Cloud platform management system can manage and configure enterprise's asset through relative interfaces to guarantee the asset's integrity and availability. And once there are some changes found in asset, the system can help managers deal with them in time.

Early-warning management

Early-warning management is a system designed to monitor the enterprise's information security. When the system find the target it will start the early-warning model to monitor and then manage the target. Today's early-warning management has gained a great progress based on the original design and has also gained some innovative improvement. Facing the dynamic attack the system can send warming signal much earlier to notice the managers to do certain risk assessment and resolve it. From negatively resolving the problem turning to today's positively processing it, the system's efficiency has been greatly increased. The early-warning can be divided into two kinds: one is that users create the warning system by themselves, including desktop warning, short message warning and e-mail warning ; the other one is that when the grade of default event is above 2 the system would automatically send early-warning signal and the enterprise can set up the grade limit according to its own using condition.

User management

User management in the cloud platform management is designed according to the grade of user. The system manager would classify the users and every user can play one or several roles and different roles have different authority. Every user can use his authority according to his role when he logins the cloud platform management system.

Report management

Report management is to analyze the actual information about enterprise's asset, time and early-warning and then show the clients through report. According to the user's demand the repot would show in different forms, but whatever form it is all of them can be downloaded.

Response management

Response management is a system to make a response to the risk and event monitoring results. Strategy base would provide the relative strategy pointing to a certain event. If the event is same with the one in the strategy base the response would be coordinated. It can attack and modified security equipment or asset, and change some service's configuration, to diminish potential threads. For those events that system cannot remove atomically the system would notify the network managers to deal with normally by sending e-mail or short message to the manager, so the system can protect network and asset security.

Data processing center

Data processing center is a very important part of cloud security management system. Data is the basis of network's operation and enterprise's using. Managers of data processing center will manage data transmission, classify data resources and arrange the software's setting. Data processing center analysis security events and assets risk through real-time monitoring. By making use of cloud computing technology to manage network platform, data processing center has gained higher efficiency and more convenience. In cloud computing technology, several virtual server can work at the same time, increasing data processing speed and the system's timeliness.

Data acquisition layer

Data acquisition layer is to collect the dynamic changes of network's lower layer's security and system log. Because network areas and equipment are various and security events are usually different from each other, so there is some difficulties ling in higher cloud computing platform's management and analysis.

Network security equipment layer

Network security equipment is the basis of cloud platform management, because it is the source of safety data, which is the foundation of network platform. The main equipment include firewall, anti-virus system, vulnerability scanner and intrusion detect system, all of which are aimed to protect cloud platform's network security.

THE DESIGN OF ENTERPRISE'S NETWORK SECURITY MANAGEMENT SYSTEM BASED ON CLOUD COMPUTING TECHNOLOGY

The aim of designing network security management system for enterprise

Network security management system is designed to cover the shortage existing in today's network technology, which can lead to data missing, making a negative effect on enterprise. The upgraded network security management system has been adjusted based on today's cloud computing technology, so it has adjustability and practicability. Users can adjust, expand and change system modules.

Schematic diagram of security management system structure for enterprise

Figure 4 is the schematic diagram of security management system structure for enterprise, which has clearly shown us the system's structure and design theory.

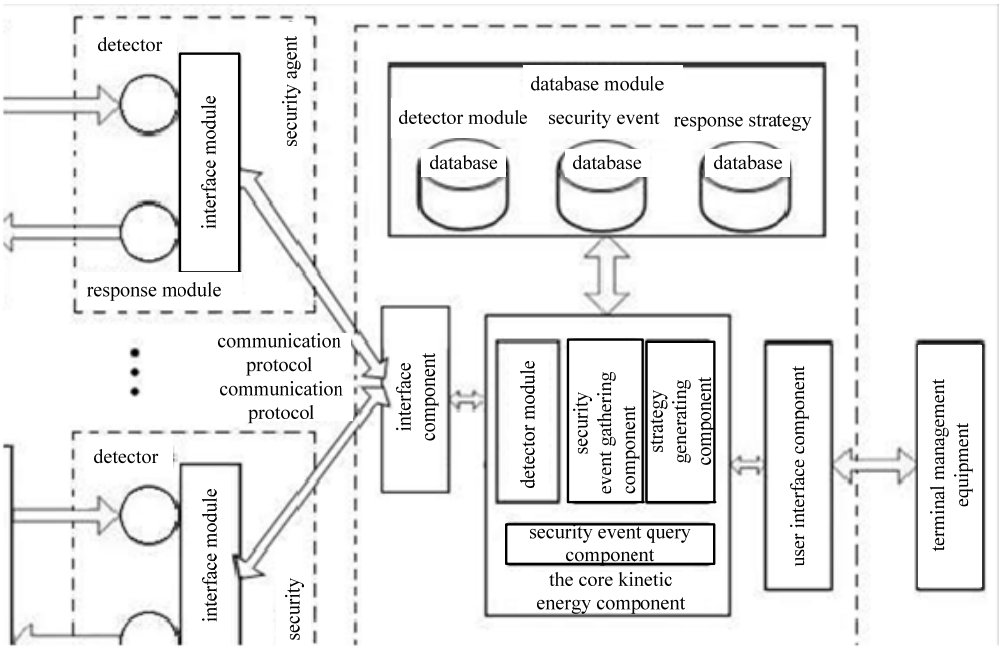

Figure 4 : Schematic diagram of enterprise's security management system structure

Enterprise's network security management is the core of enterprise's security management, which control the network's connection and data transmission. It not only can manage the network through cloud computing platform but also can process security events, efficiently reducing network risk. Enterprise's network security management has a very strong function. It only can real-time control the whole network configuration through detector but also manage the whole network through launching network orders.

CONCLUSION

Nowadays cloud computing technology is widely applied in enterprise's network security management. In the information age network has gained much great progress but also faces threads. The network security management system based on cloud computing technology covers the shortage existing in traditional network system, reduce network threat and lower the enterprise's loss caused by network shortage. However, before making full use of cloud computing technology we must completely understand it and network threat. The upgraded network security management system is designed to maintain enterprise's network security by making use of cloud computing technology's high computing speed. Cloud computing technology has been applied to maintain network security by enterprises. Cloud computing technology has gained much attention. In the future cloud computing technology will play a more and more important role. Enterprise's network security management system would gain much progress based on cloud computing technology, which not only can warn and deal with security events but also can process data rapidly.

ACKNOWLEDGEMENT

One of research results of the confirmatory study of big data in wisdom campus of colleges and universities, the subject of national “twelfth five-year” project on education and technology research in 2014.

REFERENCES

[1] Shijiang Guo, Haitao Xieli; The research and construction of unified network security management platform[J].Application Research of Computers, **9**, 92-97 **(2006)**.

[2] Zhaobin Wang, Yadi Xuning; The research of network safe operation center’s key technology[J].Computer Engineering and Design, **30(9)**, 2117-2120 **(2009)**.

[3] Weiqian, Xia Qingguo; The research of associated engine technology based on security management center[J]. Computer Engineering and Design, **28(13)**, 3085-3087 **(2007)**.

[4] Chen Siluo; The design and construction of distributed network security management platform[D].Beijing: Beijing University of Posts and Telecommunications, **(2008)**.

[5] Huang Decai, Qi Huachun; The research of Page Rank [J].Computer Engineering, **32(4)**, 145-146 **(2006)**.

[6] Wangdong, Lei, Jingsheng Lizhuang; The upgraded page sorting algorithm based on Page Rank [J]. Computer Engineering and Design, **29(22)**, 5921-5923 **(2008)**.

[7] Wang Xuesong; Lucene+Nutch Search engine’s development[M].Beijing: Post and Telecom Press, 368-375 **(2008)**.