Research on Cloud Computing Security Problem and Strategy

Wentao Liu
Department of Computer and Information Engineering, Wuhan Polytechnic University, Wuhan Hubei Province 430023, China
uddisoap@gmail.com

***Abstract*—The cloud computing is a new computing model which comes from grid computing, distributed computing, parallel computing, virtualization technology, utility computing and other computer technologies and it has more advantage characters such as large scale computation and data storage, virtualization, high expansibility, high reliability and low price service. The security problem of cloud computing is very important and it can prevent the rapid development of cloud computing. This paper introduces some cloud computing systems and analyzes cloud computing security problem and its strategy according to the cloud computing concepts and characters. The data privacy and service availability in cloud computing are the key security problem. Single security method cannot solve the cloud computing security problem and many traditional and new technologies and strategies must be used together for protecting the total cloud computing system.**

Keywords- cloud computing; cloud security; strategy

I. INTRODUCTION

The cloud computing becomes the host issue in industry and academia with the rapid development of computer hardware and software. The cloud computing is the result of many factors such as traditional computer technology and communication technology and business mode. It is based on the network and has the format of service for the consumer. The cloud computing system provides the service for the user and has the character of high scalability and reliability. The resource in the cloud system is transparent for the application and the user do not know the place of the resource. The users can access your applications and data from anywhere. Resources in cloud systems can be shared among a large number of users. The cloud system could improve its capacity through adding more hardware to deal with the increased load effectively when the work load is growing. Cloud resources are provided as a service on an as needed basis. The cloud itself typically includes large numbers of commodity-grade servers, harnessed to deliver highly scalable and reliable on-demand services. The amount of resources provided in the cloud system for the users is increased when they need more and decrease when they need less. The resource can be the computing, storage and other specification service. The cloud computing is seen as the important change of information industry and will make more impact on the development of information technology for the society. The majority of cloud computing infrastructure currently consists of reliable services delivered through data centre that are built on servers with different levels of virtualization technologies. The services are accessible anywhere in the world, with The Cloud appearing as a single point of access for all the computing needs of consumers. The cloud computing changed the style of software. The data can be stored in the cloud system and the user can use the data in any time and in anywhere. The data often stored in the private or personal system such as PC. The cloud computing can guarantee the data security and the user do not protect the data by himself again. So the cloud computing must ensure the security of data stored in the cloud system. Many companies provide the cloud computing platform such as Google, IBM, Microsoft, Amazon, VMware and EMC [1-7]. As the cloud computing system has more data which may be the private data of user, the data must not be destroyed or grabbed. Because the data in the cloud system may be important for the user, the hacker may pay more attention to get the data. The system must be protected more carefully than the traditional system. The company uses the cloud system and stores the data in it. The data can be seen by other people who are not person of company. The company must have confidence in the cloud computing if they want to store the private data in the cloud system. Governance and security are crucial to computing on the cloud, whether the cloud system is in firewall or not. The security of cloud computing is the key import problem in the development of cloud computing. The traditional security mechanism cannot protect the cloud system entirely. The cloud computing application is no boundaries and mobility and can lead many new security problems. The main security problems include data security, user data privacy protection, cloud computing platform stability and cloud computing administration.

II. CLOUD COMPUTING

The data storage and computing are not in the local computer and server but in the amount of computer distributed in the internet in the cloud computing. The cloud computing move the tasks which are implemented in the personal computer and private data center into the larger computing center which are shared with total user and distributed in the internet. It compose applications out of loosely coupled services and one service failure will not disrupt other services. The cloud computing system can be divided into two sections: the front end and the back end. They connect to each other through the internet. The front end is user who use the service provided by the back end which is the cloud section of the system. The cloud is a metaphor for the Internet, based on how it is depicted in computer network diagrams, and is an abstraction for the complex infrastructure it conceals. Cloud Computing is about the delivery of computing resources from a location other than that from the user. The computer hardware,

978-1-4577-1415-3/12/$26.00 ©2012 IEEE

software, computing resource and the service which include the resource using and management are shared fully. The services in cloud computing are ubiquitous and they can be accessed from workstations and other devices, such as cell phones. The virtualization has the ability to run multiple operating systems on a single physical system and share the underlying hardware resources. A virtual server can be serviced by one or more hosts, and one host may house more than one virtual server. If the environment is built correctly, virtual servers will not be affected by the loss of a host. Hosts may be removed and introduced almost at will to accommodate maintenance. The virtual servers in the cloud computing system can be scaled out easily and if the administrators check out that the resources supporting a virtual server are being taxed too much in the real environment and they can modify the amount of resources allocated to that virtual server. The cloud computing is developed from many technology such as parallel computing, distributed computing, grid computing and other computer technologies. The grid computing want to solve the assignment of computing and resource storage and the cloud computing want to share the computing, storage and application resource. The grid computing do not rely on virtualization as much as the cloud computing do and each individual organization maintain full control of their resources. The user need not computing and storage resource and don't provide the application in the cloud computing. The resource and server can be provided by the cloud computing. The cloud computing is divided into private cloud, public cloud and hybrid cloud according to the difference of service object. The hybrid cloud is the composition of two or more clouds and bounded by standard or proprietary technology. Hybrid clouds combine character of both public and private clouds. The private cloud is deployed in the company and the security can be made easily. Private clouds are virtualized cloud data centers inside firewall and it is a private space dedicated to system within a cloud data center. Private cloud refers to internal data centers of a business or other organization not made available to the general public. The cloud system infrastructures are owned by an organization which sells cloud services to the general public or to a large industry company. The public cloud is running in the internet and the security is very complex. Public clouds are virtualized data centers outside of firewall and the service provider makes resources available to consumer on demand over the public Internet. The cloud computing is highly virtualized and standardized infrastructures and it can give more efficient and application management. It has the character of massive scalability and it can deliver more applications to large number of users. The cloud has fault tolerant and highly reliable and can give excellent service quality. Cloud computing allows for elasticity, where capital and operational expenses for resources are only incurred when they are needed The cloud computing is on-demand service and it give computing capabilities as needed automatically. It can use the service by many machine such as desktop, laptop, PDA and mobile phone. The cloud service model include SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service). In the software as a service the consumer use the provided application and don't manage or control the network, servers storage and the application. It can reduce expenses and is easy to use and access everywhere. It share instance of a software application as a service accessible via internet browser or client based role access and sharing rules. The service provider hosts the software so the user don't need to install or manage or buy hardware for it. All they have to do is connect and use it. The examples of SaaS are Flickr, Google Docs, Siri, Amazon and Cloud Drive.

In platform as a service the consumer deploys their applications on the cloud computing system and controls their applications but they don't manage servers and storage and delivers a computing platform or solution stack as a service. It share platform for custom software application configuration, development, testing and deployment. It get the deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers and it make raw hardware made available to the user through the Internet but generally includes a specific operating system that is pre-installed and supported by the Cloud vendor. The examples of PaaS are Google App Engine, Amazon Web services. In the infrastructure as a service the consumer get access to the infrastructure to deploy their application and system but they don't manage or control the infrastructure and they control the storage and applications. It share managed pool of configurable and scalable resources such as network, middleware, database and storage servers. The examples of IaaS is Amazon Elastic Compute Cloud (EC2). The cloud has the elastic character and resource allocation can get bigger or smaller depending on demand. The cloud also has the scalability and the cloud can scale upward for peak demand and downward for lighter demand. The application can modified when adding users or when application requirements change.

There are many cloud computing systems in the market such as Google, Windows, IBM and Amazon. The Google cloud computing system include GFS (Google File System), MapReduce and Bitgtable. The GFS is a distributed file system and which contains one master server and many block servers. The file is segmented into stationary size such as 64Mb file block stored in the bock server. The MapReduce is a distributed programming mode and it can decrease the complex of programming in the cloud computing. The MapReduce include Map and Reduce operation and the Map use the Key and Value to create new Key and Value. The Reduce operation merges the same style of Key and Value. The MapReduce is not only programming mode but also efficient parallel task scheduling model. The programmer can provide their own Map function and Reduce function to process data. The Bigtable is a distributed and large scale database management system and the data is stored in the table which is divided into many rows. Many rows make a small tablet stored in the node. The Bigtable depends on the distributed cluster task scheduling, GFS and distributed locker service Chubby. Windows provide the Azure operation system which want to create cloud computing platform for the developer. The developer can make the application on the cloud server, web, PC and data center. The system supports general-purpose computing, rather than a single category of application. Amazon provide the EC2 (Elastic Compute Cloud) and S3 (Simple Storage Service). The EC2 can provide many services which ruing in the virtual machine. The user can choose different virtual machine

according to the different requirement and upload it to the S3 and call the machine interface to finish the task. The Hadoop is an open source distributed computing framework and provided by the Apache. Many network stations use it to create system such as Amazon, Facebook. The Hadoop cores are MapReduce and HDFS (Hadoop Distributed File System). The Mapreduce can make the decomposition of tasks and integration of results. The HDFS is a distributed file system and provide the base support for the storage of file in the storage node. The MapReduce contains job trackers and task trackers. MapReduce [8] is a programming model Google has used successfully is processing big data sets. A map function extracts some intelligence from raw data and a reduce function aggregates according to some guides the data output by the map. MapReduce needs a distributed file system and an engine that can distribute, coordinate, monitor and gather the results. The HDFS is a master and slaver framework and which contains data nodes and name node. The name node is a center server and mange the name space in the file system. The data node manages the data stored in it.

The cloud computing is a large scales distributed computing mode and scale economic driven mode. The large scale is the first character and it can provide more low cost service for the user. The cloud computing uses the abstract entities on the every layer function and provides cloud server for the user. The cloud server is implemented by the virtualization technology. The user can use the cloud server for the cloud system in every place and using of every terminals. The users don't worry about the concrete realization or place of cloud server. The virtualization is the charter of the cloud system and the application don't need the information of hardware platform. The cloud system can make the application in different place or different hardware. The cloud system must provide reliability server for the user and the data in the cloud center also must be protected. The cloud scale in the cloud system can be extended dynamically and can meet the growth of application and number of users. The application in the cloud also can be extended according to the number of user.

III. CLOUD SECURITY PROBLEM

The cloud system is running in the internet and the security problems in the internet also can be found in the cloud system. The cloud system is not different the traditional system in the PC and it can meet other special and new security problems. the biggest concerns about cloud computing are security and privacy [9]. The traditional security problems such as security vulnerabilities, virus and hack attack can also make threats to the cloud system and can lead more serious results because of property of cloud computing. Hackers and malicious intruder may hack into cloud accounts and steal sensitive data stored in cloud systems. The data and business application are stored in the cloud center and the cloud system must protect the resource carefully. Cloud computing is a technology evolution of the widespread adoption of virtualization, service oriented architecture and utility computing. over the Internet and it includes the applications, platform and services. If the systems meet the failure, fast recovery of the resource also is a problem. The cloud systems hide the details of service implementation technology and the management. The user can't control the progress of deal with the data and the user can't make sure the data security by themselves. The data resource storage and operation and network transform also deals with the cloud system. The key data resource and privacy data are very import for the user. The cloud must provide data control system for the user. The data security audit also can be deployed in the cloud system. Data moving to any authorized place you need it, in a form that any authorized application can use it, by any authorized user, on any authorized device. Data integrity requires that only authorized users can change the data and Confidentiality means that only authorized users can read data. Cloud computing should provide strong user access control to strengthen the licensing, certification, quarantine and other aspects of data management. In the cloud computing, the cloud provider system has many users in a dynamic response to changing service needs. The users do not know what position the data and do not know which servers are processing the data. The user do not know what network are transmitting the data because the flexibility and scalability of cloud system. The user can't make sure data privacy operated by the cloud in a confidential way. The cloud system can deploy the cloud center in different area and the data can be stored in different cloud node. The different area has different law so the security management can meet the law risk. Cloud computing service must be improved in legal protection.

IV. STRATEGY

The data stored in the cloud system can meet the problem of stolen and modified unlawfully. The data can be encrypted before stored in the cloud system. But if the data size is very large, it will need more time and computing resource. The confidential data will be treated outer people of company and the other people can access the data. Traditional techniques can protect user data privacy and security in cloud the environment to some extent. These technologies include encryption mechanism, security authentication mechanism and access control policy. Encryption mechanism depends on the reliability of the difficulty of decryption. Encryption methods include symmetric key encryption systems and asymmetric key encryption system. Asymmetric key can get high security but encryption and decryption is slow. Security authentication mechanism currently has a complete set of technical solutions. It uses the internationally accepted PKI technology, X.509 certificate standard and X.500 published standards of information technology standards. Access control policy is basic technology and is to ensure that network resources are not illegal use. It includes network access control and directory level security control. The user which can connect the cloud system includes the cloud provider, operation and maintenance personnel and the customer user. How to ensure customer data is not illegal to steal or utilize by other cloud computing providers is a major problem. The operation and maintenance personnel are responsible for data storage and backup and make the data classification management according to the level of data security. Cloud computing storage security is primarily related to data storage isolation, storage place, data recovery and data long term survivability. Once the data is stored in the cloud, the control of the data is transferred to the hands of cloud computing providers. Some unscrupulous businesses can get the customer privacy information by unfair means which is

easier from the customer. The cloud provider can transmit the customer data from the server to another server and the user can not know the data storage place. The data storage and manipulation are related to the resources of cloud center in cloud computing environment. The cloud provider is responsible for security but the monitoring and auditing for them become important problem. The cloud computing services provided for customers are difficult to achieve full transparency. Customers do not understand internal processes of cloud computing and data storage location information. The customers do not know what kind of situation data will meet if an accident occurs. Customers should have the right of the supervision and audit of cloud computing services in order to fully ensure the security of customer data. The communication of worms, virus and Trojan in cloud computing platform within the network of internal and external must be controlled. Malicious programs must be isolated promptly. Damage to the system must be repaired immediately. The data traffic in the cloud system and cloud computing system running status should be monitored in real time. The abnormal action of network and system must be detected and fixed timely. The network attack detection and defense system must be deployed in the cloud network. The service interruption and system failures because of hackers must be amended. The disaster recovery mechanism of cloud computing platform must be realized which includes important system backup and data disaster recovery. The emergency response mechanism and the emergency response capabilities for emergency case must be established and improved. The user information availability privacy and integrity must be protected. The user system and data security isolation and protection must be considered. The network data transmission security can be protected by use of data encryption and VPN technology. The management of user data encryption and key distribution mechanism must be designed carefully. The management and maintenance of user data must be safe and effective. Data backup is very important, data security recovery mechanism is also very necessary. The user's data can be promptly restored if the abnormal behavior of the system occurs. The cloud system can be considered as service oriented architecture system which hide the underlying details and provide transparent services to customers. The cloud service can be considered as the web service and the security mechanism in the service oriented architecture can be used for reference. SOA achieves interoperability between different systems and programming languages provides the basis for integration between applications on different platforms through a communication protocol. The web service has many security mechanisms such as WS-Security, WS-Reliability, WS-Trust, WS-Authorization, WS-Secure Conversation [10].

V. CONCLUSION

This paper illustrates cloud concepts and demonstrates the cloud capabilities such as scalability, elasticity, platform independent, low-cost and reliability. The security problems in the cloud system are discussed. Cloud computing has a very fast pace of development and shows good prospects and great potential. The cloud computing is related to many areas of information management and services. The data privacy issue becomes more prominent than the traditional network because the data in the cloud computing environment is greatly dependent on the network and server. There are many customers who mistrust the security and privacy of cloud computing customers and they do not want to move the data into the cloud platform from the company or private system. These problems have hindered the development of cloud computing and the security issue is the core problem. The cloud computing provider must make variety of measures to protect the security in order to effectively solve these problems.

REFERENCES

[1] Amazon Elastic Compute Cloud, http://www.amazon.com/ec2/

[2] Google App Engine, http://appengine.google.com/

[3] Saleforce, http://www.salesforce.com/platform/

[4] Microsoft, http://www.microsoft.com/,

[5] VMware, http://www.vmware.com/

[6] IBM Blue Cloud project, http://www03.ibm.com/press/us/en/pressrelease/22613.wss

[7] OpenNEbula Project, http://www.opennebula.org/

[8] Dean, J. and Ghemawat, S. 2008. MapReduce: simplified data processing on large clusters. Communication of ACM 51, 1 (Jan. 2008), 107-113.

[9] Cloud Security Alliance:http://www.cloudsecurityalliance.org/

[10] International Business Machines Corporation,Security in a Web Services World: A Proposed Architecture and Roadmap,http://msdn.microsoft.com/en-us/library/ms977312.aspx,2002