TELKOMNIKA, Vol. 11, No. 12, December 2013, pp. 7316~7323
e-ISSN: 2087-278X

Research on the Information Security Problems in Cloud Calculation's Environment

Xia Hu, Min Zhou*, Qing Xia
School of Management, China University of Mining and Technology, Xuzhou 221116, China
*Corresponding author, e-mail: xzkdzm@163.com

Abstract

With the development of technology, cloud calculation becomes a widely used technology and is regarded as the third IT revolution following the computers and the Internet. Cloud calculation benefits ordinary users to enjoy high-end IT services by making it turn into the real basic resources through IT technology, resource sharing and high concentration. While cloud calculation offers a variety of convenience, it is very vulnerable to malicious attacks of stealing service or data because the cloud stores a large amount of valuable information about users' data, privacy information and so on. While dealing with cloud computing, confidential data can be secured from the unauthorized access and internal threats. Then only after resolving its security issues, it is able to operate successfully. This paper at first introduces the concept and characteristics of cloud calculation and then elaborates the current situation of cloud calculation's security. Then it analyzes the security risks of cloud calculation. In order to make use of the cloud benefits to full extent, these risks need to be addressed first. In this paper we present the major security issues in cloud computing. Some of the countermeasures that can be implemented are also suggested.

Keywords*: cloud calculation, information security*

1. Introduction

In recent years, computer technology is developing faster and faster. At the same time, the development of Internet technology promotes the generation of many new technologies. Conceptions of cloud calculation, networking, and smarter planet and so on generate recently. Because of the new technologies, their appearance is a concern, and they develop rapidly. Currently, cloud calculation has stepped into the substantive stage of development. So its security problems also become the hotspot issues in the research of the IT field [1].

With the popularity of computers, more and more jobs need to be done on the computer. U disk becomes the essential goods of students and staffs as students have to complete the homework or papers and staff want to work in their own home. Every day before leaving the lab or the company, you need to copy all the unfinished things into U disk, which will be copied into their computers again when they get home. You take the same job at office in the morning. And sometimes, forgetting some file or program will lead to all the work uncompleted.

These situations often take place. Therefore, it is proposed that whether files and applications can be saved through the network. So long as there network exists, U disk is not needed to copy.

Cloud is actually a remote host to store users' data, including files, applications and so on. Since just storing can not satisfy our needs, the concept of cloud calculation. Then various operations of files and applications can be realized on the remote host.

Cloud calculation is an emerging concept in recent years. Users can store applications and files used frequently in a remote server, and then use any computer via the Internet to access and use these applications and files. Simply speaking, cloud calculation moves personal information from the computer to the network. As long as the Internet is approachable, all of the files can be handled through just a networking computer. In this way, all information processing and storage can be achieved through Web terminal.

Cloud calculation is the calculation mode by providing dynamic scalable virtualized resources in a service manner via the Internet. It is a pay-per-use model that provides a convenient, on-demand network access enter the shared pool of configurable computing

Received June 23, 2013; Revised July 24, 2013; Accepted August 15, 2013

resources (resources include networks, servers, storage, applications, services). These resources can be quickly provided, which simply need putting few management job or seldom interact with service providers. The concept of cloud calculation has been widely applied into the production environment, such as the domestic Ali Cloud and XenSystem of the company Cloud Valley as well as very mature Intel and IBM abroad. With the expanding scope of all kinds of cloud calculation's services, its influence is immeasurable.

Now, cloud computing is invading almost all Information Technology industries. As the number of dependents on the cloud services shoots up, the security issue has become an overwhelming problem. According to the research of the scholars, the seven famous security issues in cloud computing are privileged user access, regulatory compliance, data location, data segregation, recovery Investigative report, and long term viability [2]. Other studies have also put forward that the key security and privacy issues like access control, authentication and identification, availability, policy integration, audit and so on [3]. Some Chinese scholars have classified the security issues into six categories. The need for monitoring, the cloud server, data confidentiality, malicious insiders activities, service hijacking, issues due to multi tenancy and so on are dealt with [4]. Other studies suggested various security issues like trust, confidentiality and privacy, integrity and availability [5].

2. New Allocation Algorithm based on Ant Colony Optimization

Algorithm of ant colony is an algorithm of resources' allocation in the environment of cloud calculation [6-8]. It refers to the Map / Reduce systems that each unit cloud environments Master and Slave each unit is divided into two roles of Master and Slave. Master deploys the nodes of NameNode and JobTracker, while Slave configures the nodes of DataNode and TaskTracker.

During resource allocation, the major job of configuring the nodes in the unit and each node cluster under the jurisdiction of the unit work together to allot nodes. The nodes in all units of cloud environment are divided into two community structures. And all major nodes master JobTracker and attached nodes slave TaskTracker are respectively considered as a class. The major node is responsible for all tasks of scheduling and constituting a job. The data sources of these tasks are distributed in the mirror slices of different users which are in the resources storage of attached nodes. The main node monitors the task's execution and re-executes the failed task or deal with errors. The attached node is responsible for implementing tasks assigned by the master node. After getting the major node's distribution, the attached node starts to look for a suitable computing node for the preparation of its subordinate named storage node. Firstly, the attached node begins to detect the amount of its own computing resources. If the computing resources left can meet the usage amount for users to submit jobs, its own computing resources is allocated. If the remaining resources are insufficient to meet the minimum amount of computing resources for users to submit jobs, it begins to search for other suitable computing resources in the cloud computing environment. Ant allocation algorithm introduced below will be implemented in this part. Search work starts in a certain range in order to prevent the network overhead from increasing. If the appropriate resources still can not be found, the attached node poses to request the removal of mirror slices of users' data to the major job of configuring the nodes.

The slave node domain is regarded as an undirected graph G (V, E), where V is the collection of all the slave nodes in the regional Area and E is the network collection connecting the slave node. The cloud calculation evenly divided into several sub-regions, and then assigns the same number of ants to each region. Each group of ants only makes a research in their respective regions. Its metrics to be considered is as the following parameters.

Expected execution time: time_cost (e) refers to the elapsed time that computing resources of the end of the path e handle such work.

Network delay: delay (e), refers to the maximum network latency the path e produces.

Network bandwidth: bandwidth (e), refers to the maximum network bandwidth the path e provides.

How the diversity and preference of needs of cloud calculation resources guarantee QoS? After synthesizing the time of expected execution and network delay, the variable quantity td in (t, e) represents the usage of computing resources the end of e calculate for i in the time t.

Suppose the feature set of a virtual machine resource VM i.

$$R_i = \{r_{i1}, r_{i2}, r_{i3}, r_{i4}, r_{im}\}, m \in [1,5]$$

Here rim represents a K-dimensional diagonal matrix, respectively, CPU, the number of memory, bandwidth, costs and failure rate of the countdown.

Resource VM i describe the matrix-vector of performance's description is:

$$VM_i = \{E_{i1}, E_{i2}, E_{i3}, E_{i4}, E_{im}\}, m \in [1,5]$$

Here E_{im} indicates the eigenvalue the r_{im} corresponds to.

The description of QoS in task generally adopts the parameter indexes of time of completing task, network bandwidth, cost, reliability and so on to quantify the QoS. For example, QoS descriptions of time of completing task include the starting time, completed time, ending time, etc. When using, the time of completing all the tasks can be selected as the evaluation index.

Usually the general expected vectors of class i can be described as:

$$E_i = \{e_{i1}, e_{i2}, e_{i3}, e_{i4}, e_{im}\}, m \in [1,5]$$

Here e_{im} denote the general expectations of CPU, memory, bandwidth, etc. and satisfy:

$$\sum_{j=1}^{m} e_{ij} = 1$$

As in the cloud computing environment, the specific circumstances of resources is unknown and the network does not have a fixed topology, the distributions of structure and resources in the cloud computing environment as well as the actual situation are unpredictable. In this case, calculating the location of the computing resources and quality is unknown for the data nodes. Taking advantage of ant colony algorithm can find out the computing resources in unknown network topologies and pick out the most appropriate one or more to assign user for work until customers' needs are met. When the search begins, the slave node sends out query messages. These messages play the role of the ant in the colony algorithm. All the ants follow the principle that the more pheromones, the larger probability of nodes while the fewer pheromones, the smaller probability of nodes to select the next hop nodes and leave pheromone in the path of nodes.

3. Problems of Cloud Calculation in the History

Cloud calculation benefits ordinary users to enjoy high-end IT services by making it turn into the real basic resources through IT technology, resource sharing and high concentration. But it has diminished the users' control. Thus, data security and privacy issues will face a huge threat for individual users of cloud calculation.

While cloud calculation offers a variety of convenience, it is very vulnerable to malicious attacks of stealing service or data because the cloud stores a large amount of valuable information about users' data, privacy information and so on. Not only the malicious attackers may do harm to it, but even the legitimate users of cloud calculation who abuse resources or internal staff in the cloud computing operators are likely to harm it. Suffering severe attacks, cloud computing system will be faced with the danger of collapse and then will not be able to provide reliable services [9].

Many examples illustrate the cloud security issues can not be ignored.

In March 2011, Google Mail broke out the large-scale spill of users' data. About 150,000 Gmail users found all messages and chats in their deleted. Parts of the user accounts

were reset. Google's data showed that the number of users affected by this incident accounted for 0.08 percent of total subscriber.

In April 2011, hackers invaded the Sony's data servers in the United States. Not only the Sony's PlayStation site was intruded, but Sony PS3, music, animation cloud service network and Qriocity user profile information were stolen. It influenced 77 million users and 57 countries and regions.

In that same month, Amazon Cloud suffered the event of cloud computing security which is the most serious in the history of Amazon. That is the downtime of the Amazon data center server in a large area.

A series of security incidents show people pay more attention to cloud computing security issues in the face of devastating losses from the attack to cloud calculation.

4. Threats in the Computer Networks

4.1. Lack of Autonomy of the Core Technology of Computer Networks and Software

During the process of China's information construction, independent technical support is scare and information infrastructure in the network security is deficient. CPU chips, operating systems and databases, firewalls and gateway software, etc. used by our computers are mostly dependent on imports. The network equipment and software which our computers use are basically exotic. Due to these factors, security performance of China's computer network is greatly reduced and is considered as the glass network which is easy to hit and peep. Because of lack of independent technology, our network is in the security threats of much information, such as eavesdropping, interference, attacks, surveillance and fraud. Then network security is in a very fragile state. Meanwhile, China's network security system has many troubles in the forecasting, responding and recovery capabilities.

4.2. Hacking

Hacking into a computer system poses a great threat to the information security of the entire network [10]. Due to design or man-made causes, computer operating systems and application software systems often have some flaws or vulnerabilities. Through these vulnerabilities, an attacker can invade or control the computer system, and even destroy computer system. Usually it needs 6 months from discovering the vulnerability to exploit it further to carry out an attack. Hackers find a vulnerability of the computer network system to hacker computer systems in order to steal passwords, intercept or tamper with data, transmit the virus and the destruct the computer systems, and sometimes even cause paralysis of the entire computer. Most of the successful invasions result from the internal network while currently most of the intrusion detection systems are difficult to detect attacks from the internal network. As the information network speed of China's colleges and universities increases, hackers have sufficient bandwidth resources to attack the target host in a more subtle and easy way.

4.3. Infection of Computer Virus and Intrusion of Network Spyware

While the speed that computer viruses spread through the Internet and various storage media rapidly increase, whose harm is also growing. Especially network worm is a collection of the traditional computer viruses, worms and technologies of hacking. It has a capability of autonomous attack, which is independent on the human operators. What's more, it can install backdoors on the infected host. Aiming at multiple system vulnerabilities, it can be spread rapidly by way of self-reproduction. Then the problems of network congestion, server outages and information leakage turn out. Internet Spyware has quickly become a new threat of information security in the network. Spyware refers to the program that invading computer aims to intercept user's access to computer keyboard, screen information and network connection information without the known or explicit authorization of users. And the program is also difficult to clear from the computer. Computer viruses generally enter into the computer by way of software bundling, e-mail and visit to websites, etc.

5. Security Problems Arise by Cloud Calculation

Cloud calculation brings huge business opportunities for the companies and manufacturers [11]. These companies and manufacturers have set up departments to launch

the service of cloud calculation. As the most important asset of a company, data security should be paid enough attention by the company. So security problems of cloud calculation have been put on the agenda. As cloud-based services grow, cloud computing services will be provided by a number of chambers of service commerce instead of by only one company. If a company signed a cloud computing contract with a outsourcer, which also makes contracts with other outsourcers, and other outsourcers do the same thing, that company's confidential documents will be passed through the layers to reach the hands of a lot of businesses by the business with whom that company contract. Then the security risks raised is huge. Companies need a lot of courage to put confidential documents to the service providers of cloud calculation.

For example, the investment bank employees uses Google Spreadsheets to manage the list of employees' social security numbers, so company Google is responsible for protecting the information of these employees' social security from hackers and the internal data leaks. Banks do not need to bear this responsibility. However, there may be government investigators to order Google to hand over those social security numbers without informing the data's owners. And some companies online are even willing to share the users' sensitive data with marketing companies. Google's privacy policy states that if the company requires providing the relevant data, it should have the better reasons to meet any applicable law, regulation, legal process or enforceable demands of government. Then it will share the data with the government.

Generally speaking, the information security problems brought by cloud calculation are in the following areas.

5.1. Risks against the System Reliability

As the cloud stores a large number of users' business data, privacy information or other valuable information, it is vulnerable to get attacks. These attacks may come from the malicious attacks stealing the services or data, the legitimate users of cloud calculation abusing resources, or the internal personnel in the cloud calculation. When getting a serious attack, cloud computing system is likely to face the danger of collapse and be unable to provide highly reliable service.

5.2. Blur of the Security Boundary

The technology of virtualization is a key technology in achieving the cloud calculation. The shared data possess the borderless characteristic. And the number of servers and end-users is very large so data storages distributed. Due to the above reasons, it cannot define boundaries as clearly so the traditional network, which result to be difficult to provide adequate protection measures.

5.3. Auditability

Users themselves take the ultimate responsibility for the integrity and security of their own data. Traditional service providers are admitted to provide services for enterprises after passing the external audits and safety certification. However, as the new, high-tech service providers, some cloud computing providers refuse to accept such a review. For such providers, is for security reasons. Out of the security consideration, users will only use their services to do some grunt work rather than to complete the large-scale work.

5.4. Access of Privileged Users

Dealing with sensitive information outside of the company may be at risk, because it will bypass the corporate IT department to take the physical, logical and manual control for this information. If a company decides to use cloud computing services, it must have a good knowledge of administrators dealing with these information, and require service providers to offer the administrators' information in detail.

5.5. Data Bits

Users taking cloud computing services are not clear about the place where their data stored exactly and even the location and the country their data place in. For the sake of security, the users should ask cloud computing provider whether their data is stored in a location for specialized jurisdiction and abide by the agreement of local privacy.

5.6. Data Privacy

At first, data in the cloud is stored in the servers around the world in random. Therefore, users do not know where their data is stored in particular. In addition, after end-users deliver their data to the cloud computing providers, the priority access to the data has been changed. In other words, cloud computing providers enjoy the priority to have access. So how to ensure the confidentiality of data becomes very important.

5.7. Data Recovery

Even if the user does not know the specific location of data's storage, but cloud computing providers should tell the user what problems and situations the user data and services will appear if system is in trouble. In fact, all the data and applications without backup will emerge problems. What users need to know is that whether cloud computing providers have the ability to recover data and if so, how long it takes to recover data.

5.8. Data Isolation

In the cloud computing system, the data of all users is in a shared environment. Data encryption plays a role in the data security, but it is still not enough. Users should not only be aware whether some data is separated from other data by the cloud computing providers, but also need to know whether encryption services are designed and tested by experts. If the encryption system goes wrong, the system will have major problems and all the data will be unable to continue to use.

5.9. Investigative Support

In the cloud computing environment, because data from multiple users may be stored together and may be transferred between multiple hosts and data centers, it is hard to inquire into the improper or illegal activities. If the cloud computing providers do not have such measures, it is difficult to investigate the specific situations of violations and find out the culprit in the event of violations.

5.10. Long-term Viability

In the ideal case, the cloud computing providers will not go bankrupt or be purchased by large companies. However, users still need to confirm their data in order to ensure the security of their data. So if this problem occurs, the data will not be affected. Users need to ask the cloud computing providers how to get back their data and whether the back data can be imported into alternative applications.

6. Methods of Ensuring Cloud Computing Security Problems

Although there are a variety of concerns, cloud calculation indeed possesses the potential for development [12]. Enterprises can dramatically reduce IT costs, significantly improve efficiency and increase jobs' flexibility through the use of cloud computing services. As long as finding a complete security solution, cloud calculation can get the promotion in a larger scale [13].

For their safety, although there is not a certified solution, many solutions exist.

6.1. Encryption of the Files Saved

Files which have been encrypted by the encryption technology can be decrypted with the passwords. Even if the data is uploaded to a remote data center else, the encryption can also play a protective role. There are already encryptions strong enough to use. That is, as long as using the uncrackable passwords, no one but the owner can get access to his sensitive information.

6.2. Encryption of Emails

At present there are already a number of sophisticated encryption software, such as TrueCrypt, which can encrypt files before they are out of your control so as to play a protective role. However, because email is in the format that the voyeurs are still capable to access to reach someone's inbox, the above methods can not guarantee the security of e-mail content.

In order to ensure mail security, there are also programs that can be used, such as Hushmail, which can be used online and automatically encrypt all messages received [14].

6.3. Use of Good Services

Even if the file is encrypted, a lot of activity online on the network is still difficult to obtain protection, especially in relation to manipulate files on the Internet, not just saving the documents. This means that the users still need to seriously consider whether they need to use these services. Experts recommend to use the services with great reputation, because they generally can not take their brands to adventure. They will neither allow the occurrence of data breaches, nor will they share data with marketers.

6.4. Consideration of Business Models

Before the decision which internet service are worthy of trust is made, their profitable methods should be considered. Some Internet application services charge and some are funded by advertising. The service with fees may be safer than ad-funded services. Advertising provide economic stimulus for Internet application providers. Providers collect detailed users' data to offer data for advertisers so that they can target on advertising. Thus, the users' information may fall into the hands of criminals.

6.5. Statement of Reading the privacy

Most of Internet application service providers acknowledged in their policy that if requested law enforcement officials of government pose the demand, they will hand over the related data of users. Since almost all the privacy policies about the Internet application services have the loopholes, data can be shared in some certain circumstances, including the above situations. But users need to know what information may be shared so that you can determine which data can be stored in the cloud computing environment and which are kept by yourself.

6.6. Filtration

Websense and other companies provide a system, which can monitor which data is out of the current network to automatically prevent sensitive data from transmission. For example, identity card numbers with a unique digital arrangement by this system. Such systems can also be configured to facilitate different users in the same company to enjoy different degrees of freedom of exporting data.

7. Conclusion

Cloud calculation can bring great convenience for the users and achieve data sharing. Meanwhile its security issues can not be ignored. Only when its security is ensured, can users use cloud computing services at ease. Otherwise, they are worried about leaking their information, which will make the cloud computing service providers lose a lot of users.

There has not been a sound program to protect information in cloud computing environment as so far. Thus as long as the cloud computing service providers must work harder, they can make a set of such programs to get more customers.

Acknowledgment

This paper was supported by a grant from the Fundamental Research Funds for the Central University (NO. 2013XK01) and the Fundamental Research Funds for the Central University (NO. JG101487).

References

[1] Na Jeyanthi, Hena Shabeeb, NChSN Iyengar. A Study on Security Threats in Cloud. *International Journal of Cloud Computing and Services Science*. 2012; 1(3): 84-88.
[2] Ziyuan Wang. *Security and Privacy Issues within the Cloud Computing*. The 3rd International Conference on Computational and Information Sciences. Chengdu. China. 2011; 1: 175-178.
[3] Dawei Sun, Guiran Chang, Lina Sun, Xingwei Wang. *Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments*. 2011 International Conference on Advanced in Control Engineering and Information Science. Dali. China. 2011; 1: 2852-2856.

[4] Dimitrios Zissis, Dimitrios Lekkas. Addressing Cloud Computing Security Issues. *Future Generation Computer Systems*. 2012; 28: 583–592.
[5] Zhang XJ, MENG QC, QU WF. A Job Scheduling for Service Grid Using Ant Colony Algorithm. *Computer Engineering*. 2006; 32(8): 216-218.
[6] PAN DR, YUAN YB. Improved QoS Routing Algorithm Based on the Ant Net. *Mini-Micro Systems*. 2006; 27(7): 1169-1174.
[7] HUA Xia-yu, ZHENG Jun, HU Wen-xin. Ant Colony Optimization Algorithm for Computing Resource Allocation Based on Cloud Computing Environment. *Journal of East China Normal University (Natural Science)*. 2010; 1(1): 127-134.
[8] YIN Jue-qiong. Analysis of Situation and Problems of Cloud Computing. Computer Knowledge and Technology. 2009; 5(33): 9302-9303.
[9] YANG Yi, LAI Ying-chun. The Security Issues under the Cloud Computing Environment. *Computer Knowledge and Technology*. 2009; 5(16): 4154-4156.
[10] YANG Zhexi, XUE Huacheng. Informatization Expectation with Cloud Computing in China. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10(4): 876-882.
[11] Bo Mingxia, etc. Research on the Architecture of Cloud Computing Security. *Information network security*. 2011; 8: 79-82.
[12] Fa-Chang Cheng, Wen-Hsing Lai. Creating the Environment for the Prosperity of Cloud Computing Technology. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10(4): 864-875
[13] Teddy Mantoro, Andri Zakariya. Securing E-mail Communication Using Hybrid Cryptosystem on Android-based Mobile Devices. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10(4): 827-834.