Proceedings of the 2012 2nd International Conference on Computer and Information Application (ICCIA 2012)

Research on Key Security Strategies of Cloud Computing

Duanyang Zhao*, Qingxiang Xu, Xiaxia Hu

Zhijiang College of Zhejiang University of Technology, Hangzhou 310024, China
* Email Address: sunny@zjc.zjut.edu.cn

***Abstract*—More and more organizations and individuals outsource their storage and computing business into cloud computing, which is a representation of a movement towards the intensive, large scale specialization and economy. Cloud computing brings about convenience and efficiency, but challenges in the areas of data security and privacy protection. This paper identifies the most vulnerable security threats in cloud computing, which will enable both end users and vendors to know about the key security threats associated with cloud computing, and to know about critical analysis about the different security models and tools proposed. Key security strategies from the infrastructure, operation and security incident response relieve the common security issues of cloud computing.**

Keywords-Cloud Computing, Data Security, Privacy Protection, Security Strategy

I. INTRODUCTION

Cloud Computing represents one of the most significant shifts in information technology many of us are likely to see in our lifetimes. Reaching the point where computing functions as a utility has great potential, promising innovations we cannot yet imagine.

Customers are both excited and nervous at the prospects of cloud computing. They are excited by the opportunities to reduce capital costs, for a chance to divest them of infrastructure management, and focus on core competencies. They are excited by the agility offered by the on-demand provisioning of computing and the ability to align information technology with business strategies and needs more readily. However, customers are very concerned about the risks of cloud computing if not properly secured, and the loss of direct control over systems for which they are nonetheless accountable[1].

Cloud computing operation causes various threats and possible security issues. The internet is the main driver in all operations for cloud computing services. The internet is a host for malicious content and actions such as man-in-the-middle attacks, IP spoofing, etc. The impacts of these threats can range from data leakage to identity fraud. Data privacy and security, external threats, guest-to-cloud threats, other security issues are also becoming very important in cloud computing. As increased amounts of data are transmitted over the internet and malicious behavior continues, the protection and defense of data within the cloud will always be present[2].

The rest of the paper is organized as follows. In the next section overview of cloud computing will be introduced. Cloud Computing security issues will be discussed in section 3, the security strategies in section 4, and conclusions in last section.

II. OVERVIEW OF CLOUD COMPUTING

The anticipated benefits of cloud computing can be broadly categorized into infrastructure-oriented benefits and user-oriented benefits. The former is that an individual user would be able to realize, while the latter is that an infrastructure provider or data center operator would be able to realize across a large, aggregate set of users[3].

As with any new technology, the definition of cloud computing is changing with the evolution of technology and its services. No standard definition for cloud computing has been agreed upon, since it encompasses so many different models and potential markets, depending on venders and services. Simply, cloud computing is basically internet-based computing. The term "cloud" is used as a metaphor for Internet, and came from the cloud drawing that was used in network diagrams to depict the Internet's underlying networking infrastructure. The computation in the internet is done by groups of shared servers that provide on demand hardware resources, data and software to devices connected to the net[4].

The National Institute of Standards and Technology NIST, gives a more formal definition: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"[5].

Users of cloud computing are raised to a level of abstraction where they are hidden and relived from the details of the hardware or software infrastructures that supports their computations. This greatly simplifies the costs involved in establishing and managing the IT that is needed to meet the requirements of any business.

A. Core technologies

To better understand the security issues that are associated with cloud computing, it is important to discuss the core concepts and technologies in cloud computing. Cloud computing is based on the general principle of utility computing – providing metered services of computing resources in a similar manner to the other utilities such as electricity. The measured service-oriented perspective for computing resources can be easily understood for the hardware resources. But this perspective can also be

Published by Atlantis Press, Paris, France.

extended to software systems because they are designed and built in the form of autonomous interoperable services.

The large variety of devices that can connect to the internet, such as PDAs, mobile phones and handheld and static devices, all expanded the number of ways the cloud can be accessed. Coupled with acceptance of the browser as some sort of universal interface for even very complex systems, the potential of cloud computing could be tapped using basically any device that can load a browser. High speed broadband networks, data centers, and server farms are also critical components[4].

B. Cloud Computing Service models

The services provided by cloud computing can be categorized into three service models, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). These three models often abbreviated as the SPI Service framework (i.e. SPI is short for Software, Platform and Infrastructure) are the basis of all services provided by cloud computing:

Software as a Service (SaaS): in this model software is provided by the vendor over the net as a one-to-many model (single instance, multi-tenant architecture) as a substitute of the one-to-one typical model. Instead of users buying the software and installing it on their systems, they rent the software using pay-per-use, or subscription fee. The user exchanges the capital expense acquiring software licenses for operation expenses renting software usage. Since the application is provided over the net, usually the package includes the usage of the software itself and the utilization of the hardware it runs on, in addition to some level of support. Additional benefits of this model is centralized updating, so users don't need to worry about patching and versioning[4].

Platform as a Service (PaaS): the sophistication needed to create software that can run in the cloud entails the providers to create a development environment or platform on which these applications can be executed. The second service provided in the cloud is the utilization of the development environment itself. Users can create custom applications that target a certain platform, with tools offered by the platform provider. They then can deploy and run these applications on this platform, with full control over the applications and their configuration. Such applications may also be acquired from third parties. When using this service, users don't need, or even have the ability to manage the underlying cloud infrastructure, including servers, storage mediums and network configuration. The benefits of such a service are large, since startup companies and small teams can start developing and deploying their own software without the need to acquire servers and teams to manage them[4].

Infrastructure as a Service (IaaS): in the third service, the users are given access to elements of the computing infrastructure itself. Using internet technologies, users can utilize the processing power, storage mediums and necessary networking components provided by the vendor. Users then can run arbitrary software and operating systems that best meets their requirements, with full control and management. This is much like traditional hosting services except when done in the cloud it is possible to scale the service to conform to the changing requirements, and to offer the pay per use model. This model is very similar to utility computing where users pay for the consumption of disk space, processing power, or bandwidth that they use[4].

III. MAJOR SECURITY ISSUES IN CLOUD COMPUTING PLATFORMS

In 2011 a survey on cloud computing was distributed. Cloud.com conducted a survey in the second quarter of 2011 to determine cloud computing usage trends among IT professionals who participated in the BitNami, Cloud.com, and Zenoss open source software and user communities. The results were collected from responses of 521 individuals as to their usage. It revealed preferences for virtualization and cloud computing technologies. The number one overall reason impeding cloud computing adoption was lack of cloud computing training (43%), followed by security concerns (36%). The Apple and Google are currently driving their strategies to include education about the cloud and easing consumer security concerns. They have to stay focused on overhauling user perceptions[8]. Confusing perceptions of the cloud require the companies to enhance the user's understanding of cloud's illusion of inclusion, not confusion. For example, cloud supporters need to educate users or halt the misperception about the cloud platform. Apple chose to promote the cloud in its recent iCloud release, whereas Google downplayed the cloud in its debut. Apple's management decided to "brand it and own it for sure" according to Ipsos analyst Todd Board..

A. Threat to information privacy and confidentiality

The Internet offers the aspect of global reach. On equal measures, this platform is characterized by lack of data privacy and confidentiality[1]. Cloud computing is often invaded by malicious insiders, through service and account hacking. When unauthorized access to clients' accounts is made, erroneous manipulations can be perpetrated on data. With the frailties in security systems used by cloud service vendors such as Amazon and Microsoft Azure, several threats have cropped up. Data privacy and confidentiality on the Internet platform are done through Domain Name Server (DNS) spoofing, denial-of-service-attacks and also phishing. The use of insecure Application Programming Interfaces (APIs) enables unauthorized access to users' accounts to be a possible venture.

B. Threat of shared technology

The Internet is a shared infrastructure, a factor that has prompted the emergence of security threats in cloud computing. This sharing of the underlying cloud platforms enables the provision of online products in a scalable way, but the security issues associated with this practice are robust. This threat is often perpetrated on the disk partitions, CPU caches and the compartmentalization component. The multi tenancy offered by the Internet has attracted

Published by Atlantis Press, Paris, France.

malicious activities on these underlying components by hackers, thereby paralyzing the online operations of other users For instance, the Red and Blue Pill root kit developed by Joanna in 2006 proved to be capable of destroying the Internet and cloud computing platforms such as CPU caches and GPUs[1].

C. Threat to data loss and leakage

The exposure of clients' data to other cloud computing users can lead to data loss and leakage[9]. This threat is perpetrated through improper encoding and encryption of data files or encryption. The cloud service providers may fail to seek the consent of data clients when deleting or altering electronic records. In addition, the lack of secure software keys and frail authentication processes can also lead to loss or leakage of sensitive corporate data in the cyberspace[9]. According to the CSA, the current data retention strategies that are used over the Internet platform are not efficient[1]. Unauthorized access to user accounts has become a common practice due to the use of weak access control and API infrastructures. Data transmission has suffered the threat of network access through spoofing. In this process, hackers often monitor user network access and spoof MAC addresses.

Companies like Google, Amazon, and Microsoft are the forerunners in using cloud computing technology. Just like any form of technology it has had its fair share of challenges: ranging from government intervention in foreign countries and attacks from hackers and they have been able to rise up from these challenges by securing and encrypting their servers through the SLL technologies and upgrading of their firewalls. With the support of stable operating systems like UNIX, Google has been able to secure its E-mail system. With the flexibility and fixing of the security loopholes, cloud computing technology has proven to be a great success[8].

D. Other security issues

It includes insecure interfaces and APIs, malicious insiders, and an unknown risk profile. APIs are used as the bridge between a user and their services. Because a lot of activity occurs on these interfaces the possibility of vulnerabilities is high. General cloud services depend upon the security of these basic APIs to maintain their own security and availability[1].

A malicious insider is a major threat to consumers of cloud services. The centralized location of consumers' data poses a major issue if a person with malicious tendencies infiltrates a cloud providers system. If the providers' security procedures for physical and logical access controls do not meet those of the consumers it can allow a malicious employee on the providers' side to collect and or modify data that belongs to a consumer. This kind of situation clearly creates an attractive opportunity for an adversary ranging from the hobbyist hacker, to organized crime, to corporate espionage, or even nation-state sponsored intrusion[1].

The data stored in a cloud is a distributed file system. It is a need to solve the problem of how to verify the correctness of data on the basis of the dynamic operation of data blocks. Cloud is an open sharing environment of storage and computing resources. Cloud services generally provide digital identity to the user, and the different services of the same users need to manage different encryption and signature information. Difficult to manage hybrid cloud composed of multiple public and private clouds, the user identity the corresponding key.

IV. SOME KEY SECURITY STRATEGIES OF CLOUD COMPUTING

There are fundamental principles of security that cloud computing needs, in order to make guarantees to its users: confidentiality, integrity, availability, authenticity, and information security and users privacy. Cloud computing technology users need to be assured of confidentiality when using the system. Confidentiality involves assuring the customer that there information will not be disclosed with or without their authority. This is important to the companies that use cloud computing and transact their business online and it could involve the use of credit cards. This security principle needs to be considered since business and organizations will lose their customers if not assured of the security of their personal information[8].

Cloud security infrastructure service is a cloud-based software service layer, to provide a common information security services for all types of cloud applications, to be an important means to support cloud applications for user security objectives [9]. Cloud user identity management services: the identity of the supply, cancellation and authentication process. In cloud environment, the identity federation and single point of login can more easily share user identity information and authentication services of cooperation between the cloud enterprises, and reduce the run overhead of repeated certification. The process of cloud identity federation management should protect the privacy of user digital identity. Because digital identity information may be shared between multiple organizations, security management in the various stages of its life cycle is a challenging problem. The federated identity-based authentication process in a cloud computing environment has high security needs

Cloud access control services: their implementation rely on how to immigrate traditional access control model (such as role-based access control, attribute-based access control model and the mandatory/discretionary access control model, etc.) and authorization policy language standards (XACML, etc.) to the cloud environment after expansion. Because the need of compatibility of all enterprises and organizations in the cloud resources is increasing, federation license is the important issue in service security framework of cloud access control.

Cloud audit services: because the lack of safety management and proof ability to clear security responsibility, cloud users may require service providers to provide the necessary support. It is very important for a third party to implement the cloud audit. Cloud audit services must provide for the audit event list with all the evidence and the credibility description of the evidence. If

Published by Atlantis Press, Paris, France.

the evidence does not disclose other user information, data forensic methods are required special design.

Cloud password service: because users of cloud need widespread data encryption and decryption operation, the services of cloud password emergence. Addition to the services of the most typical type of encryption and decryption algorithm, secret key and certificate management and distribution in cryptographic operations are the basis of cloud security services. Cloud password services not only simplify the design and implementation of a cryptographic module, and make use of cryptographic techniques more concentrated, normative, and easier to manage for the users.

Cloud security application services: Cloud security application services closely integrated with the needs of users, such as protection cloud services of DDOS attack, cloud web filtering and anti-virus applications, content security service, security event monitoring and early warning cloud services, cloud spam filtering and prevention. Cloud computing provides large-scale computing power and massive storage capacity, improves the security event correlation analysis, virus protection and other aspects of the performance. It can be used to build vast information processing platform for security incidents, and to enhance the security ability of the entire network.

Trusted Cloud Computing: With cloud computing further development and growth, a variety of security issues have gradually understood and a variety of solutions have been proposed. In a complex computer system, it is difficult to solve all problems with software. With advantage of the hardware chip and trusted computing support, a solution may try to support trusted computing. In the cloud environment, trusted computing base (TCB) protect the secret of the users, the providers of the infrastructure and service, achieve integrity measurement, and implement the proof of the credibility of the identification of the parties and the software, so that trusted cloud computing based on the credible class is constructed [10].

V. CONCLUSIONS

Cloud computing is a kind of computing paradigm that can access conveniently a dynamic and configurable public set of computing resources (e.g. server, storage, network, application and related service), provided and published rapidly and on-demand with least management and intervention. The prevalence of cloud computing is blocked by its security to a great extent. To contribute some effort to improving the security of cloud computing, we surveyed the main existing security models of cloud computing, and summarized the main security risks of cloud computing from different organizations. Finally, we gave some security strategies against these common security issues of cloud computing. In the future, we will fulfill these security strategies with technology and management ways.

REFERENCES

[1] Cloud Security Alliance. Top Threats to Cloud Computing, Version 1.0 (2010). Retrieved October 15, 2009, from https://cloudsecurityalliance.org/topthreats.

[2] Huiming Yu, Nakia Powell, Dexter Stembridge, Xiaohong Yuan, Cloud Computing and Security Challenges. In proceedings of the 50th Annual Southeast Regional Conference. (2012) March 29, Bryant, Tuscaloosa.

[3] Craig A. Lee. A Perspective on Scientific Cloud Computing, In proceedings of the 19th ACM International Symposium on High Performance Distributed Computing. (2010) June 20, New York, USA.

[4] Kamal Dahbur, Bassil Mohammad, Ahmad Bisher Tarakji. A Survey of Risks, Threats and Vulnerabilities in Cloud Computing, In proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications. (2011) April 18, Amman, Jordan.

[5] P. Mell, T. Grance. The NIST definition of cloud computing. National Institute of Standards and Technology. Special Publication 800-145. September 2011. Gaithersburg, USA.

[6] Yi Wei, M. B. Blake, Service-Oriented Computing and Cloud Computing: Challenges and Opportunities. IEEE Internet Computing. 14, 6 (2010)

[7] Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud security and privacy, O'Reilly Media, Sebastopol, CA (2009).

[8] David Teneyuca, Internet cloud security: The illusion of inclusion, Information Security Technical Report. 102, 10(2011).

[9] Feng Dengguo, Zhang Min, Zhang Yan, etc. Study on Cloud Computing Security. Journal of Software, 2011, 22(1):1−83.

[10] Yang Jian, Wang Haihang, Wang Jian. Survey on Some Security Issues of Cloud Computing. Journal of Chinese Computer Systems, 2012, 33(3): 42-49.

Published by Atlantis Press, Paris, France.