Research On Cloud Computing And Security

Ting-ting Yu
Internet Of Things Department
Wuxi Institute Of Technology
Wuxi, China
e-mail: yutt@wxit.edu.cn

Ying-Guo Zhu
Internet Of Things Department
Wuxi Institute Of Technology
Wuxi, China
e-mail: zhuyg@wxit.edu.cn

***Abstract*—Cloud computing is the hottest technology discussed on the internet recent years, which is considered as the trend in the development of the Internet. With the further application of cloud computing , security issues became one of the focuses concerned by people . From a practical point of view, this article combined with cloud computing framework, focus on the threats to cloud computing environments, as well as appropriate countermeasures**

Keywords- Cloud computing; Architecture; Threat Countermeasures

I. INTRODUCTION

Cloud computing is a flexible, cost- effective and proven delivery platform for providing business or consumer IT services over the Internet. NIST describes cloud computing as "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".

In march 2006, Amazon release Elastic Compute Cloud (EC2) service. In the same year, Eric Schmidt (Google CEO) first proposed Cloud Computing in SES San Jose 2006. February 1, 2008, IBM announced the establishment of the world's first Cloud Computing Center (Cloud Computing Center) for Chinese software companies in China Wuxi Taihu New Town Science and Education Industrial Park. March 5, 2010, Novell and Cloud Security Alliance (CSA) announced a vendor-neutral program, called "TTrusted Cloud Initiative".

From a practical point of view, this article combined with cloud computing framework, focus on the threats to cloud computing environments, as well as appropriate countermeasures.

II. CLOUD ENVIRONMENT ARCHITECTURE

The cloud computing model consists of five characteristics, three delivery models, and four deployment models. The five key characteristics of cloud computing are: location-independent resource pooling, on-demand self-service, rapid elasticity, broad network access, and measured service. These five characteristics represent the first layer in the cloud environment architecture (see Figure1).

The three key cloud delivery models are infrastructure as a service (IaaS), platform as a service(PaaS), and software as a service (SaaS).

<table>
<tr><th>Layer</th><th colspan="3">Cloud Computing Components</th></tr>
<tr><td rowspan="4">Five Characte -ristics</td><td colspan="3">On-demand self-service</td></tr>
<tr><td colspan="3">Broad network access</td></tr>
<tr><td>Resource</td><td colspan="2">Rapid elasticity</td></tr>
<tr><td colspan="3">Measured Service</td></tr>
<tr><td>ThreeDelivery model</td><td>IaaS</td><td>PaaS</td><td>SaaS</td></tr>
<tr><td rowspan="2">Four Deployment</td><td colspan="2">Public</td><td>Private</td></tr>
<tr><td colspan="2">Community</td><td>Hybrid</td></tr>
</table>

Figure 1: Cloud Environment Architecture.

- Infrastructure (storage, computation and network capabilities) as a Service (IaaS), basically consisting on the deliverance of virtual machines (VMs) to an IaaS provider, who can rise or shrink the number of VMs so as to offer fast and easy scalability according to variable workloads.
- Platform (development, service lifecycle, etc. support tools) as a Service (PaaS), offering facilities to develop software products and host them in third-party infrastructures.
- Software as a Service (SaaS),where the user buys a subscription to some on-line software.

Among these three, IaaS is, arguably, the most established cloud service model, already offering a wide variety of products and advanced capabilities: automated scalability, pay-per-use, and on-demand provisioning are some of the most relevant.This model represents the second layer in the cloud environment architecture.

Cloud deployment models include public, private, community, and hybrid clouds. A cloud environment that is accessible for multi-tenants and is available to the public is called a public cloud. A private cloud is available for a

978-0-7695-4818-0/12 $26.00 © 2012 IEEE
DOI 10.1109/DCABES.2012.28

particular group, while a community cloud is modified for a specific group of customers. Hybrid cloud infrastructure is a composition of two or more clouds (private, community, or public cloud). This model represents the third layer in the cloud environment architecture.

Kamara and Lauter present two types of cloud infrastructure only, namely private and public clouds. The infrastructure that is owned and managed by users is in the private cloud. Data that is accessed and controlled by trusted users is in a safe and secure private cloud, whereas the infrastructure that is managed and controlled by the cloud service provider is in a public cloud. In particular, this data is out of the user's control, and is managed and shared with unsafe and untrusted servers.

III. THE STATUS OF CLOUD COMPUTING

At present, ICT giants ,such as Google, Amazon, Microsoft, IBM, are actively promoting research and deployment of cloud computing services and applications, including Google App Engine, Amazon's Elastic Compute Cloud EC2 and Simple Storage Service S3Microsoft's Azure cloud platform, IBM's "Blue cloud".

Although cloud service providers can offer benefits to users, security risks play a major role in the cloud computing environment. According to the IDC report released at the end of 2009,the three market challenges faced by cloud computing services are security, stability, and performance. Ranking of the three challenges faced by cloud computing service is the same as that of IDC in 2008 findings . In November 2009, the survey of the ForresterResearch company indicates that 51% of small and medium enterprises believe that security and privacy issues is the main reason why they haven't used cloud services.

This shows that safety is the first consideration when customers choose the cloud. because of its high concentration of users, information resources, security consequences and risks associated with Cloud computing have more than raditional application. In 2009, Google, Microsoft, Amazon, the company's cloud computing services have a major fault, resulting in thousands of customer information services affected, which further increased the industry's concerns about application security in the cloud.

IV. CLOUD COMPUTING SECURITY RISKS AND COUNTERMEASURES

In this section, we have analyzed the security threats present in the cloud and their mitigation based on our experience of implementing the cloud.

A. VM-Level attacks

The cloud computing is based on VM technology. For implementation of cloud, a hypervisor such as VMWare vSphere, Microsoft Virtual PC, Xen etc. are used. This threat arises because of the vulnerabilities appearing in these hypervisors due to some facts being overlooked by developers during the coding of these hypervisors.

The threat arising due to VM-Level vulnerabilities can be mitigated by monitoring through IDS (Instruction Detection System)/IPS (Intrusion Prevention System) and by implementing firewall.

B. Abuse and Nefarious use of cloud computing

This threat arises due to relatively weak registration systems present in the cloud computing environment. In cloud computing registration process, anyone having a valid credit card can register and use the service. This facilitates anonymity, due to which spammer, malicious code authors and criminals can attack the system.

This type of threat can be mitigated in following ways:

- By implementing stricter registration process and validation process.
- By credit card fraud monitoring and coordination.
- Detailed introspection of user's network traffic.
- Network blocks through monitoring public black lists.

C. Insecure Interfaces and APIs

Customers use a set of software Interfaces or APIs to interact with cloud services. The provisioning, management, orchestration and monitoring of the cloud service are generally done using these interfaces .If the weak set of interfaces and APIs are used, this may expose organizations to various security threats, such as anonymous access, reusable tokens or password, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring, and logging capabilities.

To mitigate the above threats, the security model of cloud provider interfaces should be analyzed. Strong authentication and access controls should be implemented. Encryption should be used for transmission of content and, dependency chain associated with the API should be clearly understood.

D. Malicious Insides

When the lack of knowledge about cloud vendor programs and processes the risk of malicious insiders will increase. Enterprises should know about information security of vendors and management policies, forcing them to use strict supply chain management as well as to strengthen close cooperation with suppliers. At the same time, should also have clearly specifies instructions in legal contracts to regulate carriers deal with these hidden processes such as user data in the cloud.

E. Sharing Technology

IaaS vendors in infrastructure is not safe to provide the strong isolation in a user schema. Cloud computing provider uses virtualization technology to narrow this gap, but due to the possibility of security vulnerabilities , companies should supervise the unauthorized changes and behavior, and promote the implementation of patch management and strong user authentication.

F. Data loss or leakage

Data loss or leakages have an adverse effect on the business. The brand or reputation is completely lost and the customers' morale and trust are eroded. This data loss or

leakage may be due to insufficient authentication, authorization and audit controls, inconsistent use of encryption and software keys, disposal challenges, a data center reliability, and disaster recovery.

The threats arising due to data loss or leakage can be mitigated by encrypting and protecting integrity of data in transit, analyzing data protection at both design and runtime, implementing strong key generation, storage and management. Contractually demanding provider to wipe persistent media before it is released in to pool and contractually specifying provider backup and retention strategies.

G. Account or service Hijacking

Phishing, fraud, and exploitation are wellknown issues in IT. The cloud adds a new dimension to this threat: "if an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites.Your account or service instances may become a new base forthe attacker".

To mitigate the above threats, sharing of account credentials between users and services should not be allowed, multi-factor authentication techniques should be used wherever possible, strict monitoring should be done to detect unauthorized activity, and security policies, as well as SLAs of the cloud provider, should be clearly understood.

H. Unknown risks

Knowing the security configuration used by users, including versions of the software, code updates, security practices, vulnerability profiles, intrusion attempt or security design.Find out who is sharing the user's infrastructure, to get network intrusion logs as soon as possible and related information in an attempt to redirect.

V. CONCLUSION

With the rapid development and wider application of cloud computing technology, cloud computing will face more security risks. Although there are several standards organizations in the study of cloud computing security industry on cloud computing security solution and there is no uniform standards and solutions. Many companies have introduced cloud computing security products, but innovation is obvious enough, but usually only address one small aspect of the problem. In order to cope with the ever-changing security threats, we need to constantly explore new cloud security solutions, and gradually establish an effective cloud security system, the maximum extent possible to reduce the security threats of the cloud computing system, to improve the continuity of the cloud services to protect the cloud computing applications for health and sustainable development.

REFERENCES

[1] (NIST), http://www.nist.gov/itl/cloud/

[2] H. Takabi, J.B.D. Joshi and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security & Privacy, 8(6),2010, pp. 24-31

[3] S. Kamara and K. Lauter, "Cryptographic cloud storage", FC'10: Proc. 14thIntl.Conf. on Financial cryptograpy and data security,2010, pp. 136-149

[4] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, 34(1), 2011, pp 1-11

[5] J. Viega, "Cloud computing and the common man",Computer, 42, 2009, pp. 106-108

[6] Meiko Jensen ,Jorg Sehwenk et al., "On Technical Security,Issues in cloud Computing "IEEE International conference on cloud Computing, 2009

[7] M.Jensen ,N.Gruschka et al., "The impact of flooding Attacks on network based services "Proceedings of the IEEE International conference on Availiabilty,Reliability and Security (ARES) 2008

[8] Armbrust ,M. ,Fox, A., Griffth, R., et al "Above the clouds: A Berkeley View of Cloud Computing" , UCB/EECS-2009-28,EECS Department University of California Berkeley, 2009