A Research On Cloud Computing Security

Omkar Shori
M.C.A (VI Semester)
Kalinga University Village-Kotni
Kalinga University Village-Kotni

DEPARTEMENT COMPUTER SCIENCE
Mr Rahul Chawda
Near Mantralaya Naya Raipur-492101
Near Mantralaya Naya Raipur-492101

Abstract— **This paper gives an overview on cloud computing security. To clarify cloud security, a definition and scope of cloud computing security is presented. An ecosystem of cloud security is shown to illustrate what each role in industry can do in turn. Then security impacts of cloud security for both customers and operators are analyzed. To overcome challenges from cloud security, many state-of-the-art technical solutions, e.g., continuation protection mechanism, IDM, data security, and virtualization security are discussed. Finally, best practices on perspective of operator are summarized and a conclusion is conducted.**

Keywords-Cloud security; Cloud Computing; data security; Security as a service

ACKNOWLEDGMENTS

First We would like to thanks our Coordinator, Mr Rahul Chawda, for all his help about the project. Indeed, he has guided us in order to write the report, and has helped us to take the right decision about our project. Thanks to him, we have done a project in time without missing important points of the project. Moreover, we would like to thank him with his help about the report. In fact, for international student, we don&#39;t have the same method of doing a project, so, Mr.Rahul Chawda has helped us in this way. Finally, and in generally, we would like to thank Kalinga university Raipur,Chattisgarh.

I. INTRODUCTION

Cloud Computing represents one of the most significant shifts in information technology in our lifetimes. The development of Cloud computing brings revolution to the current business model. Cloud computing has become a new hot topic in the Information Communication Technology (ICT) industry. Everyone is looking forwards to the potential development of the new market. In principle, Cloud computing has been defined by National Institute of Standards and Technology (NIST) [1] as a model for enabling convenient, ondemand 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 cloud provider interaction. The actual term "cloud" borrows from telephony in that telecommunications company [2], which until the 1990s offered primarily dedicated point-to-point data circuits, began offering Virtual Private Network (VPN) services with comparable quality of service but at a much lower cost. Cloud computing technologies can be implemented in a wide variety of architectures, under different service and deployment models, and can coexist with other technologies and software design approaches. Cloud computing can be identified by five key features, three service model (IAAS, SAAS, PAAS) [3], three deploy model (public, private, and hybrid) [4].

The new features of cloud computing, such as multitenancy [5], resource sharing [6], remote data storage [7] etc have not just challenged to the current security system, but also revealed new security problems. It is vital to ensure appropriate security measurement study on the impact of cloud computing so as to deliver a controllable cloud computing services to the governments, enterprises and individuals without the security threat.

Unfortunately, there are only limited efforts towards focusing on cloud computing security (cloud security in short) on behalf of operators. It is therefore necessary to conduct a series of technical researches on cloud security from the perspective of operators, while driving the development and introducing it to the industry. This paper presents security problems encountered in cloud computing, and has a research on many technical solutions for cloud security problems.

The rest of this paper is organized as follows. Section II proposes a definition and scope of cloud computing security, gives an overview on cloud security industry, and discusses security impacts of cloud computing both on the customers and operators. Section III discusses many security technical solutions to overcome the challenges from cloud security, including continuation, IDM, data security, interface security, virtualization security, Security as a service (SaaS) [8], etc. Then section IV, a conclusion and cloud security best practices on the perspective of operators will be conducted.

II. CLOUD COMPUTING SECURITY

This section discusses contents on cloud computing security, including definition and scope of cloud computing security, roles in cloud security industry, and threats of cloud security both to the customers and to operators.

A. The definition and scope of Cloud security

Many operators now are contributing their own understandings of cloud computing. It is inevitable for the operators to face security problems in cloud computing, also called cloud security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. That is, cloud security focuses on security issues from Cloud computing system, such as privacy protection, data encryption and resources availability under security threat. We should ensure that all these issues are being properly addressed and resolved in order to ensure the sustainability of the cloud computing development environment. Note that cloud security is not to be confused with "cloud-based" security service over the traditional threat. This security service can be enhanced with the cloud computing, protecting agains DDOS, Trojan, Virus and Spam etc more effectively than ever.

B. Cloud security Industry

In order to hinder security incidents from occuring at maximum extent, the consistitution of cloud security industry should be clarified. Three roles of cloud security industry are shown as follows.

Cloud Vendors. Many cloud service providers, such as Amazon [9], IBM [10], and Microsoft [11] have already proposed deployment solution for the cloud computing security, to improve cloud computing service platform competency, service continuity and user data security. Most of them are based on ID authentication, audit, and data encryption.

Operators. From operator perspective, there are two approaches from the security of cloud computing. On the one hand, they can achieve central control over the network through synthesizing the existing security systems with cloud computing technology. On the other hand, they can develop cloud computing security services for their customers. Some network operators, have started such service to their customers.

Security Vendors. Traditional IT security vendors, entering cloud computing market, contribute their cloud based security solutions and products, which can be categorized into two types. One sees the “cloud” from the server perspective, while the other one sees the “cloud” from the client’s perspective. The idea of former is to stop the security threats from the server side, before they reach the client side. This can be further understood as building a huge lists system. The latter is working on the traditional approach. That is to apply terminal clients for security measures.

For these three roles in cloud security industry, operators enable to drive cloud security to provide customers security services, which operators cooperate with security vendors to offer customers both client side and server side cloud security services or applications by the advantages of operators, and at the same time combine with ID authentication, audit, and data encryption solutions of the cloud vendors to offer customers end-to-end security solutions in cloud computing.

C. Security impact of cloud computing on the customers

Customers are both excited and nervous at the prospects of Cloud Computing. They are excited by the agility offered by the on-demand provisioning of computing and the ability to align information technology with business strategies. However, customers are also very concerned about the risks of Cloud Computing if not properly secured. The user‘s privacy, business information and trade secret are under threats as the follows.

Data compromise. There are many ways to compromise data. Deletion or alteration of records without a backup of the original content is a typical example. Loss of an encoding key may also result in destruction. Customers, including governments, organizations, companies, and individuals, storing their data in the CSPs’ data center which cannot guarantee a high reliability of the service, will face a risk of data compromise and service interruption.

Data leaks. The customer’s data is first accessed by the CSP instead of themselves. Customer‘s data and applications are facing double security risks, i.e. threats from CSP and threats from other unauthorized users, which brings the threat of data leaks. In multiple tenant environments, customers typically share components and resources with other customers that are unknown to them, which can be a major drawback for some applications and requires a high level of assurance for the strength of the security mechanisms used for logical separation. Without a safe logical separation, customers‘ data may be accessed by others, resulting in data leak.

Data wiping. Customer’s data should be erased completely when requested or unsubscribed. Without a complete erase mechanism, customer’s data would be stolen and then obtained by latter customers in cloud environments.

D. Security impact of cloud computing on operators

Operators have an advantage to become CSPs. As CSPs, they are excited by the opportunities to reduce capital costs and cheered for a chance to divest themselves of infrastructure management, and focus on core competencies. Meanwhile, operators have to face the challenges coming with the flexibility and scale increase. The bigger the scale of a cloud service is, the more attacks it will face. A big scaled cloud service failure revelant to security will be much worse than a traditional system failure. They should enhance security mechanism in the cloud to keep cloud computing service operating well. Therefore, the items in the following should be paid attention by the operators.

Bad compatibility, portability and interoperability. Customers have rights to change cloud service providers but the data may not be compatible between clouds. Operators should provide public and standard cloud platform to provide compatible and interoperable service for users.

Availability of cloud service. Malware may exploit cloud system vulnerabilities and then occupy a big amount of resources service or get administrator right to attack operator or other users.

Cloud resource abuse. Operators could offer their customers the illusion of unlimited compute, network, and storage capacity. By abusing the relative anonymity behind these registration and usage models, spammers, malicious code makers, and other criminals have been able to conduct their activities with relative impunity. It is difficult to trace back and find the attacker. Bad user could make use of power computing capability of cloud to crack passwords with little cost. It is very difficult for operator to detect and prevent such behaviors in real time.

Identity and access control breach. The cloud computing can provide high level of virtualization and centralization. Operators should provide business customers better access control and enhanced identity management policies to follow the rapid expansion of cloud service. **Encryption algorithm cracks.** Due to frequent occurrence of user privacy information leak incidents in recent years, current encryption methods and key management methods have been cracked. They have to be strengthened to protect customer’s data in the multi-tenant environment.

Unsecure API and interface. It is well known that cloud API bridges between customer, i.e., user handset, and cloud service infrastructure. If cloud API is infected by malware, user privacy data probably is stolen and removed, and operator would not provide XaaS (IaaS, PaaS, or SaaS) services to customers.

Virtual machines cross contamination. Virtualization may bring flexibility and improve capability. But currently there is no method developed to isolate and protect the VMs, which gives rise to a cross contamination

Data retraction. Regulation and legal requirement may request electrical evidence be stored and available. How to retract necessary information to meet the regulation and legal request is another challenge.

III. SECURITY SOLUTIONS

In order to overcome challenges from cloud security, stateof-the-art technical solutions relevant to cloud security should be considered. This section shows four typical aspects of technical solutions for operators as shown on Table I.

TABLE I. CLOUD SECURITY SOLUTIONS

Security solutions	Description
Continuation Mechanism	The security solution of service migration from non-cloud platform to cloud platform.
IDM	Simplified authentication management for cloud environment and end-to-end trustable access technology.
Data security	Data transmission, data isolation, data wiping
virtualization security	Virtualization Machine Monitoring (VMM) security, Virtual Machine (VM) security, and virtualization network security.

A. *Continuation of service from traditional platform to cloud platform.*

Enterprises are looking to cut costs and gain agility by migrating primary business applications to cloud infrastructure. However, for operators, migrating those applications to cloud infrastructure is proving to be a challenge. Applications are not usually well suited to cloud infrastructure. What's more, managing business workloads in the cloud often requires new IT techniques and brings new risks. Therefore, it is necessary to clarify application migration solutions.

B. *Identity and access Management*

Unauthorized access to information resources in the cloud has become increasingly an area of concern for enterprises. One terrible issue is that the existing identification and authentication framework may not naturally migrate to the cloud, i.e., extending or changing the existing framework to support cloud services is difficult. Meanwhile, many unknown threats will emerge in cloud system. Therefore, traditional identity management and authentication schemes should be upgraded or extended in order to strength security level. Advanced solutions as follows should be considered. Identity federation [12] is one solution that can be accomplished in a number of ways, such as with the Security Assertion Markup Language (SAML) standard [13], the OpenID standard (SSO) [14], or eXtensible Access Control Markup Language (XACML) [15]. Advanced authentication scheme is another solution, to identity management. For example, biometrics authentication [16] is more robust than traditional password typing way. Customers may use biometrics sensor, e.g, phone camera, mic, or fingerprint scanner to acquire their biometric features with uniqueness (face image, palmprint, fingerprint, voice etc), for authentication. In addition, multiple factor authentications should also be taken into account. In future, simplification of identity management and end-to-end trust access mechanism should be considered.

C. *Data security*

Data Transmission. It is inevitable that data transmission is conducted in cloud computing service. Data transmission security is a common issue not only in non-cloud system, but also in cloud. In order to maintain confidentiality, completeness and availability of network data transmission, encryption schemes, e.g., IPSec, VPN, and SSL are able to be incorporated within cloud computing system. These schemes can provide an encryption channel to cloud computing system.

Data isolation. To implement information separated among cloud users, the scheme like physical isolation, virtualization, and data label can be employed to isolate different customers (tenancy) data and configuration information, so as to protect privacy and security of user data. **Data wiping.** Customer's residual data in cloud infrastructure, e.g., disks without data wiping mechanism raises leak of their sensitive information. Therefore, data wiping in cloud is necessary and its steps can be done. Firstly, delete customers' data on the media, e.g., disks in a cloud data center, once the customers have permitted to remove them. Secondly, An inspection should be conducted on these disks, in order to ensure the data has been wiped. Thirdly, the wiped media, e.g., disks then can be redeployed and reused. In case of the disks in which data can not be wiped, they should be destroyed.

D. *Virtualization security*

Virtualization seems to be a core technique in cloud computing, with promises of cost savings, ROI, and ease of administration. It can help organizations optimize their application performance in a cost-effective manner. But, like any new technology, there are security risks inherent in virtualization that needs to be addressed.

Access control. Access control in virtual environment refers to the practice of restricting entrance to a resource to authorized VM. A well designed access control policy will make the physical resources being used appropriately and communication between VMs and between VM and VMM more trustworthy. There are six control statements which should be considered to ensure proper access control management: 1) Control access to information; 2) Manage user access rights; 3) Encourage good access practices; 4) Control access to network services; 5) Control access to operating systems; 6) Control access to applications and systems.

Virtual Machine Monitor. In VM system architecture, Virtual Machine Monitor (VMM) is the most important layer that should be heavily facilitate with security mechanisms to protect VMs running. VMs are able to be protected through security control layer which is a set of security functionalities separated from VMM. By this way, VMM will become thinner and could delegate all security tasks to security control layer.

Virtual Firewall. A Virtual Firewall (VF) is a firewall deployed and running entirely within a virtual environment and which provides the packet filtering and monitoring. The VF can be realized in a traditional software firewall on a guest virtual machine already running, or it can be a purpose-built virtual security appliance designed with virtual network security in mind, or it can be a virtual switch with additional security capabilities, or it can be a managed kernel process running within the host VMM.

IV. CONLUSION AND BEST PRACTICES

Cloud computing brings not only challenges but also evolutions for the information security. The evolutions are reflected in three aspects: the technology ideas, the industrial development and the security regulation strategies.

The evolution of technology ideas are pointing to balanced security requirements among users, service providers and even government regulators. Both users and the cloud providers have their own security requirements. Those requirements may conflict in some way. How to compromise the requirements of data security and privacy protection is one of the toughest tasks we need to fulfill. These balances between requirements need us to refresh our technical ideas.

The evolution of the industry development is reflecting the change of information security from focusing on product development to focusing on services. It is necessary to push information security products to migrate from product development to service and infrastructure development. A standardized service and infrastructure platform can help to solve various security issues users are facing.

The regulations and management evolution is reflecting the change of market regulator's focusing point. Compared with traditional regulation which concerns on core network infrastructure protection, the regulators are more focusing on big scale attacks in the cloud. It is worth mentioning that all changes are not revolutions of the existing technical strategies but improvements.

Under this circumstance, some best practices are proposed for operators to overcome shortcoming in cloud security as follows.

1. Operators should consider how to safely evolve to cloud platform from traditional one with keeping continuity of service.
2. Operators should pay attention how to solve problem related to data security in their own clouds, for example, solutions for security transmission, security isolation, security storage, and data recovery.

3.Operators should provide customers a sophisticated virtualization security solution to keep IaaS service working well.

4. Operators should monitor any attacks against their cloud services, and figure out a way to incident response.
5. Operators should identify application security problems for different service models (SaaS, PaaS, and IaaS) respectively.
6. Operators should consider legal issues and customers benefit carefully when they are to deploy any security schemes in cloud.

ACKNOWLEDGMENT

This project is supported by the National Natural Science Foundation of China under Grant No71172134 and the National Science & Technology Major Projects under Grant No 2012ZX03002001.

REFERENCES

[1] P. Mell, T. Grance. The NIST Definition of Cloud Computing, Vol 15, 2009. http://csrc.nist.gov/groups/SNS/cloud-computing.

[2] Cloud computing. http://en.wikipedia.org/wiki/Cloud_computing. [3] Security guidance for critical areas of focus in cloud security computing V3.0 http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf [4] Top Threats to Cloud Computing, V1.0, Cloud Security Alliance, 2010, https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[5] A. Sirisha, G. G. Kumari. "API access control in cloud using the role based access control model." 2nd International Conference on Trendz in Information Sciences & Computing , 2010, p.135-137.

[6] D. W. Chadwick, M. Casenove. "Security APIs for My Private Cloud: Granting access to anyone, from anywhere at any time." 2011 IEEE 3rd International Conference on Cloud Computing Technology and Science, 2011, p.792-798.

[7] A. Mana, A. Munoz, J. Gonzalez. "Dynamic security monitoring for Virtualized Environments in Cloud computing." 1st International Workshop on Securing Services on the Cloud (IWSSC), 2011, p.1-6.

[8] Amazon Web Services, http://aws.amazon.com.

[9] Cloud computing security. URL :http://en.wikipedia.org/wiki/Clo ud_comput ing_security.

[10] IBM, "Implementing Gentry's Fully-Homomorphic Encryption

Scheme" , http://researcher.ibm.com/

[11] Reference Architecture for Private Cloud.http://social.technet.micro soft.com/wiki/contents/articles/6765.private-cloud-security-model-legaland-compliance-issues.aspx.

[12] Y. He, B. Wang, X. Xiao, M. Jing. Identity Federation Broker for Service Cloud, 2010 International Conference on Service Sciences, 2010, p.115-120.

[13] F. Nie, F. Xu, R. Qi. SAML-based single sign-on for legacy system, 2012 IEEE International Conference on Automation and Logistics, 2012, p. 470-473.

[14] Y. Chen, B. Wu, B. Xia, L. Shi, C. Ward, N. Aravamudan, K. Bhattacharya. Design of web service single sign-on based on ticket and assertion. 2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce, 2011, p.297-300.

[15] B. Lang, N. Zhao, K. Ge, K. Chen. "An XACML Policy Generating Method Based on Policy View." Third International Conference on Pervasive Computing and Applications, 2008, p.295-301.

[16] A. Kong, D. Zhang and M. Kamel, "A survey of palmprint recognition", Pattern Recognition, 2009,Vo. l42, No. 7, p. 1408-1418.