Security Threats to Cloud Computing

Prashant Kumar, Department of Computer Science & Engineering, Tula's Institute, The Engineering and Management College, Dehradun
Lokesh Kumar, Department of Computer Science & Engineering, Tula's Institute, The Engineering and Management College, Dehradun
Kapil Kumar, Department of Computer Science & Engineering, GRD Institute of Technology, Dehradun
Sachin Kumar, Department of Computer Science & Engineering, Tula's Institute, The Engineering and Management College, Dehradun
Sohan Lal, Department of Computer Science & Engineering, Tula's Institute, The Engineering and Management College, Dehradun

ABSTRACT

Cloud computing offer a new and exciting way of computing with various service models that facilitates different services to the users. As all the data of an enterprise processed remotely and exchanges via different networks. Security is an essential parameter and the service provider must ensure that there is no unauthorized access to the sensitive data of an enterprise during the data transmission. This paper analyzes various security threats to cloud computing. To offering good service, cloud computing service providers must avoid these threats.

Keywords: *cloud computing, security, data privacy, SaaS.*

I. INTRODUCTION

Cloud computing is Internet-based computing, whereby share resources, software and information, are provided to computers and devices on-demand, like the electricity grid [1]. "Cloud" is a virtualized pool of computing resources. It can manage a variety of different workloads. These workloads may include the batch of some back-end operations and user-oriented interactive applications. A cloud supports highly scalable programming model that provide redundancy and self-healing, so that workload can be recover from a variety of inevitable hardware/software failure. Cloud is a real-time monitor resources usage, rebalance the allocation of resources when needed [2].

Cloud computing collects all the computing resources and manages them automatically through software. The historical data and present data are integrated to make the collected information more accurate. In this way cloud computing provides more intelligent service to the users. The users are not bothered about how to buy a server or solution. Instead they can buy the computing resources on the internet according to their need.

However cloud computing emerge as promising technology in order to provide the services remotely. But there are many security issues in cloud computing. For example in February, 2010, the Amazon network host service, S3 (Simple Storage Service) was broken down for 4 hours. This made people think about the security of cloud computing again. Since Amazon provides S3, it has attracted a lot of entrepreneur on Web 2.0 put their website on the data center of Amazon to save a large hardware investment [8]. So the service of cloud computing is not stable and believable. Security is still a major concern in cloud computing and one of the reason that's why cloud computing is still not admitted by the users.

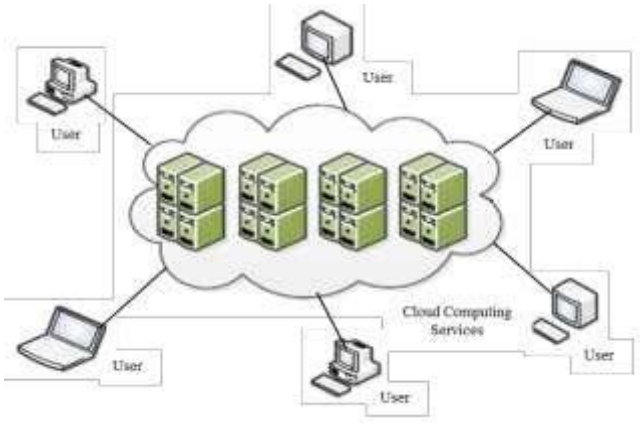

Figure 1. Basic architecture of a cloud computing network

Rest of the paper is organized as follows: Section 2 describes the cloud computing service model. Section 3 describes about the security threats in SaaS. Security issues

in PaaS are discussed in section 4. In section 5 addressed the security challenges in IaaS service model. Section 6 will concludes the paper.

II. SERVICE MODEL

There are many views on the service model in the cloud computing. But the basic ones are:

A. Software-as-a-Service (SaaS)

SaaS is a software deployment model where applications are remotely hosted by the application or service provider and made available to customers on demand, over the Internet. The SaaS model offers the customers with significant benefits, such as improved operational efficiency and reduced costs. SaaS is rapidly emerging as the dominant delivery model for meeting the needs of enterprise IT services. However, most enterprises are still uncomfortable with the SaaS model due to lack of visibility about the way their data is stored and secured [5]. According to the Forrester study, "The State of Enterprise Software: 2009," security concerns are the most commonly cited reason why enterprises are not interested in SaaS. Consequently, addressing enterprise security concerns has emerged as the biggest challenge for the adoption of SaaS applications in the cloud [7]. There are vulnerabilities in the applications and systems availability may lead to the loss of valuable information and sensitive data or may be the money. These concerns discourage the enterprises to adopt the SaaS applications in the cloud. So a service provider must address these issues.

B. Platform-as-a-Service (PaaS)

In PaaS, the development environment is provided as a service. PaaS offers an integrated set of developing environment. By this a developer can develop their applications without having any idea what is going inferior to the service and can deliver it to the users through Internet and servers.

C. Infrastructure-as-a-Service (IaaS)

Now there is no need to purchase the servers or data centers for applications deployment. IaaS completely change the way of application deployment. Now just buy all resources needed as a fully outsourced service. For example just go to an IaaS provider, like Amazon Web Services, get a virtual server and pay only for the resources the use.

D. Hardware-as-a-Service (HaaS)

According to Nicholas Carr [3], "the idea of buying IT hardware or even an entire data center as a pay-as-you-go subscription service that scales up or down to meet your needs. But as a result of rapid advances in hardware virtualization, IT automation, and usage metering and pricing, I think the concept of hardware-as-a-service, let's call it HaaS, and may at last be ready for prime time." This model is advantageous to the enterprise users, since they do not need to invest in building and managing data centers.

III. SECURITY ISSUES IN SAAS

A. Data Security

The sensitive data of an enterprise exist within the enterprise state line, but in the SaaS model the enterprise data is stored at the SaaS service provider end. So the additional security checks must be implemented by the SaaS service provider to ensure the data security. This may include the robust encryption and authorization systems to control the unauthorized access to the data. Some assessments to authenticate the security of the enterprise data at the SaaS service provider end are [5]:

- Cross-site Scripting (XSS)
- Access control weaknesses
- OS and SQL injection flaws
- Cookies manipulation
- Hidden filed manipulation
- Insecure storage and insecure configuration

If any weakness is sensed in these test leads to access of sensitive data by an unauthorized person.

B. Network Security

In a SaaS model, enterprise data processed and stored at the SaaS service provider's end. The network, which is used for data transmission, must be very secure in order to prevent the unauthorized data access. This comprises the use of strong network traffic encryption techniques such as Secure Socket Layer (SSL) and the Transport Layer Security (TLS) for security. However some illegal and malicious user s may deed the flaws of the network to sniff the data packets. Some assessments like network penetration and packet analysis, insecure SSL trust configuration and session management weaknesses can be run to authenticate the security of the enterprise data at the SaaS service provider end.

C. Data Integrity

One of the most crucial issues in any system is data integrity, which can be achieved easily in an individual system by maintaining various database constraint and transactions. Most databases support ACID (atomicity, consistency, isolation and durability) and can preserve the data integrity. But there are multiple databases and multiple applications exist in the distributed systems. In order to maintain data integrity in a distributed system, transactions across multiple data sources need to be handled correctly in a fail safe manner. This can be done using a central global transaction manger. Each application in the distributed system should be able to participate in the global transaction via a resource manager. Although there are standards available for managing data integrity with web services such as WS-Transaction and WS-Reliability, these standards are not yet mature [5] and not many vendors have implemented these. Most SaaS vendors expose their web services APIs without any support for transactions. Also, each SaaS application may have different levels of availability and SLA (service-level agreement), which further complicates management of transactions and data integrity across multiple SaaS applications.

D. Data Confidentiality Issues

Data confidentiality is a major concern in cloud computing. As in cloud computing involves the sharing or storage of enterprise data on isolated or remote servers governed service providers and accessed via internet. The entire data may be stored with a single cloud provider or with many cloud providers. So when an enterprise or an individual store the information with the cloud, confidentiality and privacy issues are arise. Some of the findings related to the confidentiality issues are [5]:

- Cloud computing has substantial implications for the privacy of personal information as well as for the confidentiality of business and governmental information.
- A user's privacy and confidentiality risks vary significantly with the terms of service and privacy policy established by the cloud provider.
- For some types of information and some categories of cloud computing users, privacy and confidentiality rights, obligations, and status may change when a user discloses information to a cloud provider.
- Disclosure and remote storage may have adverse consequences for the legal status of protections for personal or business information.
- The location of information in the cloud may have significant effects on the privacy and confidentiality protections of information and on the privacy obligations of those who process or store the information.
- Legal uncertainties make it difficult to assess the status of information in the cloud as well as the privacy and confidentiality protections available to users.

EPCA (Electronic Communications Privacy Act of 1986) offers some protections against government access to electronic mail and other computer records held by third parties. The privacy protections available under ECPA for the wide range of cloud computing activities are difficult to predict. Indeed, simply identifying all cloud computing applications would be a significant challenge by itself. Factors that may affect the proper applications of ECPA to cloud computing activities include

- The precise characterization of the activity as a communication or as a storage, complicated by the recognition that an activity can move from being a communication to being store communication depending on time and possibly other factors.
- Whether the information in question is content or non-content (e.g., header or transaction information).
- The terms of service established by the cloud provider.
- Any consent that the user has granted to the provider or others.
- The identity of the service provider, for example, if the cloud provider is itself a government agency, the provider's obligation would be different from those of a non-governmental cloud provider, and the rights of users would be different.

E. Data Backup

The SaaS service providers must guarantee that all enterprise data is properly backed up to ensure the recovery in case some disaster. In case of disaster, to prevent unauthorized access to the enterprise data, the service providers must use the strong encryption techniques. To validate the security of the data back

up the service providers may run insecure storage and insecure configuration test.

IV. SECURITY IN PAAS

In PaaS, the development environment is provided as a service. PaaS offers an integrated set of developing environment. By this a developer can develop their applications without having any idea what is going inferior to the service and can deliver it to the users through Internet and servers. People needs to build the application on the top of the platform, the service provider might give some control to the developer. But any security below the application level such as host and network intrusion prevention will still be in the scope of the provider and the provider has to offer strong assurances that the data remains inaccessible between applications. PaaS is intended to enable developers to build their own applications on top of the platform. As a result it tends to be more extensible than SaaS, at the expense of customer-ready features. This tradeoff extends to security features and capabilities, where the built-in capabilities are less complete, but there is more flexibility to layer on additional security.

Applications sufficiently complex to leverage an Enterprise Service Bus (ESB) need to secure the ESB directly, leveraging a protocol such as Web Service (WS) Security [9]. The ability to segment ESBs is not available in PaaS environments. Metrics should be in place to assess the effectiveness of the application security programs. Among the direct application, security specific metrics available are vulnerability scores and patch coverage. These metrics can indicate the quality of application coding. Attention should be paid to how malicious actors react to new cloud application architectures that obscure application components from their scrutiny. Hackers are likely to attack visible code, including but not limited to code running in user context. They are likely to attack the infrastructure and perform extensive black box testing. The vulnerabilities of cloud are not only associated with the web applications but also vulnerabilities associated with the machine-to-machine Service-Oriented Architecture (SOA) applications, which are increasingly being deployed in the cloud [5].

V. SECURITY IN IAAS

IaaS completely change the way of application deployment. Now just buy all resources needed as a fully outsourced service. For example just go to an IaaS provider, like Amazon Web Services, get a virtual server and pay only for the resources the use. With IaaS the developer has better control over the security as long as there is no security hole in the virtualization manager. Also, though in theory virtual machines might be able to address these issues but in practice there are plenty of security problems [10, 11]. The other factor is the reliability of the data that is stored within the provider's hardware. Due to the growing virtualization of 'everything' in information society, retaining the ultimate control over data to the owner of data regardless of its physical location will become a topic of utmost interest. To achieve maximum trust and security on a cloud resource, several techniques would have to be applied [12]. The security responsibilities of both the provider and the consumer greatly differ between cloud service models.

Amazon's Elastic Compute Cloud (EC2) [13] infrastructure as a service offering, as an example, includes vendor responsibility for security up to the hypervisor, meaning they can only address security controls such as physical security, environmental security, and virtualization security. The consumer, in turn, is responsible for the security controls that relate to the IT system including the OS, applications and data [14].

VI. CONCLUSION

In this paper we presents an analysis of security attacks in cloud computing. It is mandatory to the service provider to assure the security of the enterprise confidential data. However the service providers protect the data against the various security threats to ensure the user's data security. To offering good service, cloud computing service providers must avoid these threats. Beside these, practically there is many other security concern related to the security of the data.

REFERENCES

[1] http://en.wikipedia.org/wiki/Cloud_computing.
[2] G. Boss, P.Malladi, D. Quan, L. Legregni, H. Hall, HiPODS,www.ibm.com/developerworks/websphere/zones/hipods/
[3] http://www.roughtype.com.
[4] J. Yang, Z. Chen, "Cloud Computing Research and Security Issues"
[5] S. Subashini, V.Kavitha, " A survey on security issues in service delivery models of cloud computing", Elsevier Journal of Computer Applications, Vol 34, pp. 1-11, 2011.
[6] M. Jensen, J. Schwenk, N. Gruschka, L. Lo Iacono "On Technical Security Issues in Cloud Computing", IEEE International Conference on Cloud Computing,

pp. 109-115, 2009.

[7] Lo H, Wang R, Garbani J-P, Daley E, Iqbal R, Green C, Forrester report. The State of Enterprise Software: 2009.

[8] Shuai Zhang, Shufen Zhang, Xuebin Chen, Xiuzhen Huo, "Cloud Computing Research and Development Trend", Second International Conference on Future Networks, pp. 93-97, 2010.

[9] Web Service (WS) Security, Oracle, http://www.oracle.com/ technology/tech/soa/mastering-soa-series/part2.htmlS.

[10] CR Attanasio, "Virtual machines and data security", In Proceedings of the Workshop on Virtual Computer Systems, New York, pp. 206–209, 1973.

[11] S Gajek, L Liao, J. Schwenk, "Breaking and Fixing the Inline Approach", In SWS '07 Proceedings of the ACM Workshop on Secure Web Services, New York, pp. 37–43, 2007.

[12] M Descher, P Masser, T Feilhauer, AM Tjoa, D Huemer, "Retaining Data Control to the Client in Infrastructure Clouds", In International Conference on Availability, Reliability and Security, pp. 9–16, 2009.

[13] Amazon. Amazon Elastic Compute Cloud (EC2), /http://www.amazon.com/ ec2/S, 2010.

[14] A Seccombe, A Hutton, A Meisel, A Windel, A Mohammed, A Licciardi, "Security Guidance for Critical Areas of Focus in Cloud Computing, v2.1. Cloud Se curity Alliance, 2009, 25