Security issues in SaaS of cloud computing

C. Lakshmi Devi, D. Kanyakumari, Dr K. Venkataramana

Abstract: Cloud computing is becoming increasingly popular in distributed computing environment. Locking at the impact it as on numerous business applications as well as this makes IT resources available,known as cloud computing ,opens opportunities to small ,medium- sized ,and large companies. Data storage and processing using cloud environments is becoming a trend worldwide. Software as a Service (SaaS) one of major models of cloud which may be offered in a public, private or hybrid network. If we look at the impact SaaS has on numerous business applications as well as in our day to day life, we can easily say that this established technology is here to stay. Cloud computing can be seen as Internet-based computing. By using a cloud computing specimen can have positive as well as negative effects on the security of service consumer's data. Many of the important features that make cloud computing very attractive, have not just challenged the existing security system, but have also exposed new security risks. In this paper we are going to showcase some major security issues of current cloud computing environments.

KEYWORDS: Cloud Computing, Software as a Service, Security Challenges

1 INTRODUCTION

A lot has been written and spoken about Cloud Computing technology, by IT experts, industry and business leaders and independent experts. At a high-level, we believe that security of SaaS based systems can be broken six levels: cloud, network, sever, user access, application, anddata. That sidethere should be coordination between these levels, as well as a system that can collect all of this data in order to make sense of it. There also needs to be process and training put in place we are believers in a layered model for security, because each layer today can be a target .By systematically securing each layer, your software as a services solution will be better secured. According to Gartner [1], cloud computing can be defined as ''a style of computing, where massively scalable IT-enabled capabilities are delivered 'as a service' to external customers using Internet technologies. According to the Sercombe [2] and National Institute of Standards & Technology [3], guidelines for cloud computing, it has four different deployment models namely private, community, public and hybrid as well as three different delivery models that are utilized within a particular deployment model. These delivery models are the SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service). These models form the core of the cloud and they exhibit certain key characteristics like on demand self-service, broad network access, resource pooling, measured service and rapid elasticity. Our main area of concern in this paper is the Software as a service (SaaS).

2 SECURITY ISSUES IN SAAS

In Software as a Service (SaaS) model, the client has to depend on the service provider for proper security measures. The provider must ensure that the multiple users don't get to see each other's data. So, it becomes important to the user to ensure that right security measures are in place and also difficult to get an assurance that the application will be available when needed [4]. While using SaaS model, the cloud customer will, by definition, be substituting new software applications for old ones. Therefore, the focus is not upon portability of applications, but on preserving or enhancing the security functionality provided by the legacy application and achieving a successful data migration [2] The SaaS software vendor may host the application on his own private server or deploy it on a cloud computing infrastructure service provided by a third-party provider (e.g. Amazon, Google, etc.). The use of cloud computing coupled with the 'pay-as-you-go' approach helps the application service provider reduce the investment in infrastructure services and enables it to concentrate on providing better services to the customers. The cloud provider might, additionally, replicate the data at multiple locations across countries for the purposes of maintaining high availability. Most enterprises are familiar with the traditional on- promise model, where the data continues to reside within the enterprise boundary, subject to their policies. Cloud computing providers need to solve the common security challenges being faced by traditional communication systems. At the same time, they also have to deal with other issues inherently introduced by the cloud computing paradigm itself. In the following section, the SaaS security issues have been categorized as traditional and new cloud specific security challenges, for sake of convenience. Figure 1 shows the various security issues in SaaS model which are discussed in the paper.

2.1 Traditional Security Challenges

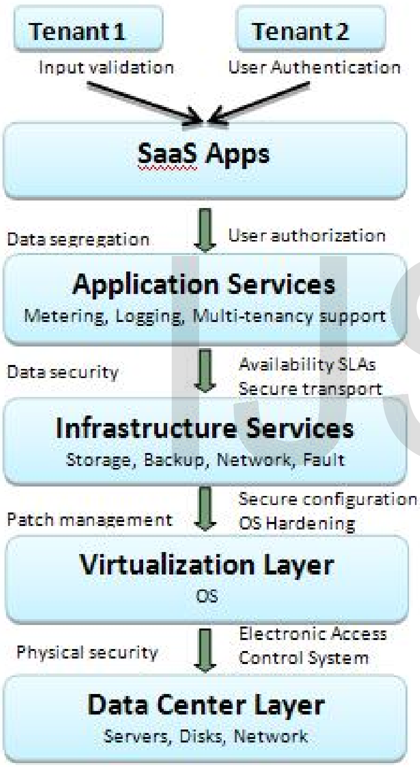

Figure 1: Security Issues in SaaS

- *D.kanyakumari,2nd year MCA ,KMMIPS, Tirupati* mailId:kanyaakhila@gmail.com
- C.Lakshmi Devi, 2nd year MCA, KMMIPS, Tirupati,mailIdl:lakshmidevia12345@gmail.com
- Dr. K.Venkataramana, Dept. of MCA, KMMIPS, Tiirupati, mailId:ramanakv4@gmail.com

2.1.1Authentication and authorization

The authentication and authorization applications for enterprise environments may need to be changed, to work with a safe cloud environment. Forensics tasks may become much more difficult since the investigators may not be able to access system hardware physically. The design proposed by Pratap Murukutla [5] allows user to use a single set of credentials. They have proposed a solution with de-facto standards of open authorization in which there is a trust party auditor which maintains all the credentials and cloud provider can uniquely distinguish one user from other. The model proposed in the literature [6] verifies user authenticity using two-step. Verification, which is based on password, smartcard and out of band (i.e. strong two factors) authentication. In addition, the scheme also provides mutual authentication, identity management, session key establishment, user privacy and security against many popular attacks; however the formal security proofing hasn't yet been formalized.

2.1.2 Availability

The availability ensures the reliable and timely access to cloud data or cloud computing resources by the appropriate personnel. The availability of cloud service providers is also a big concern, since if the cloud service is disrupted; it affects more customers than in the traditional model. For instance, the recent disruption of the Amazon cloud service in the year 2011, took down a number of websites including Reedit, Foursquare, and Quota.The SaaS application providers are required to ensure that the systems are running properly when needed and enterprises are provided with services around the clock. This involves making architectural changes at the application and infrastructural levels to add scalability and high availability. Resiliency to hardware/software failures, as well as to denial of service attacks, needs to be built from the ground up within the application. At the same time, an appropriate action plan for business continuity and Disaster Recovery (DR) needs to be considered for any exigencies as per the guidance provided by [2]. This is essential to ensure the safety ofthe enterprise data while maintaining minimal downtime for the enterprises. With Amazon [7] for instance, the Amazon Web Services (AWS) API end points are hosted on the same Internet-scale, world-class infrastructure that supports the Amazon retail site. Standard Distributed Denial of Service (DDoS) mitigation techniques such as synchronous cookies and connection limiting are used. To further mitigate the effect to potential DDoS attacks, Amazon maintains internal bandwidth that exceeds its provider-supplied Internet bandwidth.

2.1.3Data confidentiality

Confidentiality refers to the prevention of intentional or unintentional unauthorized disclosure of information. Confidentiality in cloud system is related to the areas of intellectual property rights, covert channels, traffic analysis, encryption, and inference. Cloud computing involves the sharing or storage of information on remote servers owned or operated by others, while accessing through the Internet or any other connections. Cloud computing services exist in many variations, including data storage sites, video sites, tax preparation sites, personal health record websites and many more. The entire contents of a user's storage device may be stored with a single cloud provider or with multiple cloud providers. Whenever an individual, a business, a government agency, or any other entity shares information in the cloud, privacy or confidentiality questions arise.

2.1.4Virtual Machine Security

Is the control of administrator on host and guest operating systems? Current Virtual Machine Monitor (VMMs do not offer perfect isolation. Many bugs have been found in although the global adoption of virtualization is a relatively a recent phenomenon, threats to the virtualized infrastructure are evolving just as quickly [8]. The hypervisor and virtual machines used in cloud providers may also have vulnerabilities, as exemplified by [11]. Such vulnerabilities represent an even more serious problem in multi-tenant environments, where compromise of even a single virtual machine can affect all users on the same physical server. Virtualization is one of the main components of a cloud. But this poses major security risks. Ensuring that different instances running on the same physical machine are isolated from each other is a major task of virtualization which is not met completely in today's scenario. The other issue all popular VMMs that allow escaping from VM. Virtual machine monitor should be 'root secure', meaning that no privilege within the virtualized guest environment permits interference with the host system. Some vulnerability has been found in all virtualization software which can be exploited by malicious, local users to bypass certain security restrictions or gain privileges. For example, the vulnerability of Microsoft Virtual PC and Microsoft Virtual Server could allow a guest operating system user to run code on the host or another guest operating system. Vulnerability in Virtual PC and Virtual Server could allow elevation of privilege. Cloud providers, therefore, might need to reconsider traditional security concerns from different angles.

2.2 Cloud Specific Security Challenges

2.2.1 Information Security

In a traditional on-premise application deployment model, the sensitive data of each enterprise continues to reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies. However, in the SaaS model, the enterprise data is stored outside the enterprise boundary, at the SaaS vendor end. Consequently, the SaaS vendor must adopt additional security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees. This involves the use of strong encryption techniques for data security and fine-grained authorization to control access to data.

2.2.2 Network Security

In a SaaS deployment model, sensitive data is obtained from the enterprises, processed by the SaaS application and stored at the SaaS vendor end. All data flow over the network needs to be secured in order to prevent leakage of sensitive information. This involves the use of strong network traffic encryption techniques such as Secure Socket Layer (SSL) and the Transport Layer Security (TLS) for security. In case of Amazon Web Services (AWS), the network layer provides significant protection against traditional network security issues, such as MITM (Man-In-The-Middle) attacks, IP spoofing, port scanning, packet sniffing, etc. For maximum security, Amazon S3 is accessible via SSL encrypted endpoints.

2.2.3 Resource Locality

In a SaaS model of a cloud environment, the end-users use the services provided by the cloud providers without knowing exactly where the resources for such services are located, possibly in other legislative domains. This poses a potential problem when disputes happen, which is sometimes beyond the control of cloud providers. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in much enterprise architecture [112]. The European Union has issued a Directive 95/46/EC to protect the user privacy at all costs [13].

2.2.4 Cloud standards

To achieve interoperability among clouds and to increase their stability and security, cloud standards are needed across different standard developing organizations. For example, the current storage services by a cloud provider may be incompatible with those of other provider. In order to keep their customers, cloud providers may introduce so called ‘‘sticky services’’ which create difficulty for the users if they want to migrate from one provider to the other, e.g., Amazon’s S3 is incompatible with IBM’s Blue Cloud or Google storage. Cloud Security Alliance (CSA), Distributed Management Task Force [14], Storage Networking Industry Association [15], Open Grid Forum [16], Open Cloud Consortium [17] and Organization for the Advancement of Structured Information Standards [18], and so forth. To promote the wide use of cloud computing, these standards bodies need to sit down and work together to establish common standards. Possible ‘‘Inter-cloud’’ standards in the following domains are needed to increase cloud interoperability and free data movement among clouds:

– Network architecture, – Data format, – Metering and billing, – Quality of Service, – Resource provisioning, – Security, identity management and privacy. As stated, there are many general computing standards that may be reused in the cloud, but for the moment, there

2.2.5Data Segregation

Multi-tenancy is one of the major characteristics of cloud computing. As a result of multitenancy, multiple users can store their data using the applications provided by SaaS. In such a situation, data of various users will reside at the same location. Intrusion of data of one user by another becomes possible in this environment. This intrusion can be done either by hacking through the loop holes in the application or by injecting client code into the SaaS system. A client can write a masked code and inject into the application. If the application executes this code without verification, then there is a high potential of intrusion into other’s data. A SaaS model should therefore ensure a clear boundary for each user’s data. The boundary must be ensured not only at the physical level but also at the application level. The service should be intelligent enough to segregate the data from different users. A malicious user can use application vulnerabilities to hand- craft parameters that bypass security checks and access sensitive data of other tenants.

2.2.6 Data Access

Data access issue is mainly related to security policies provided to the users while accessing the data. In a typical scenario, a small business organization can use a cloud provided by some other provider for carrying out its business processes. This organization will have its own security policies based on which each employee can have access to a particular set of data. The security policies may entitle some considerations, wherein, some of the employees are not given access to certain amount of data [19]. These security policies must be adhered by the cloud to avoid intrusion of data by unauthorized users [20].The SaaS model must be flexible enough to incorporate the specific policies put forward by the organization. The model must also be able to provide organizational boundary within the cloud because multiple organization will be deploying their business processes within a single cloud environment.

2.2.7Web application security

SaaS is software deployed over the internet and/or is deployed to run behind a firewall in local area network or personal computer. The key characteristics include Network-based access to, and management of, commercially available software and managing activities from central locations rather than at each customer's site, enabling customers to access application remotely via the Web. SaaS application development may use various types of software components and frameworks. These tools can reduce time-to-market and the cost of converting a traditional on premise software product or building and deploying a new SaaS solution. Examples include components for subscription management, grid computing software, web application frameworks and complete SaaS platform products. One of the ''must-have'' requirements for a SaaS application is that it has to be used and managed over the web. The software which is provided as a service resides in the cloud without tying up with the actual users. This allows improvising the software without inconveniencing the user. Security holes in the web applications thus create a vulnerability to the SaaS application. In this scenario, the vulnerability can potentially have detrimental impact on all of the customers using the cloud. The challenge with SaaS security is not any different than with that of any other web application technology. However one of the problems is that traditional network security solutions such as network firewalls, network intrusion detection and prevention systems (IDS & IPS), do not adequately address this problem. Web applications introduce new security risks that cannot effectively be defended against at the network level, and do require application leveldefenses. The Open Web Application Security Project has provided the ten most critical web applications security threats.

2.2.8 Data breaches

Since data from various users and business organizations lie together in a cloud environment, breaching into the cloud environment will potentially attack the data of all the users. In the Verizon Business breach report blog it has been stated that external criminals pose the greatest threat (73 percent), but achieve the least impact (30,000 compromised records), resulting in a Virtualization vulnerability [21].

3 CURRENT SECURITY SOLUTIONS

The Open Web Application Security Project (OWASP) maintains list of top vulnerabilities to cloud-based or SaaS models which is updated as the threat landscape there are several research works happening in the area of cloud security. Several groups and organization are interested in developing security solutions and standards for the cloud. The Cloud Security Alliance (CSA) is gathering solution providers, non- profits and individuals to enter into discussion about the current and future best practices for information assurance in the cloud [11]. The Cloud Standards website collects and coordinates information about cloud-related standards under development by the groups changes [10]. The Open Grid Forum publishes documents to containing security and infrastructural specifications and information for grid computing developers and researchers [13]. The best security solution for SaaS applications is to develop a development framework that has tough security architecture. One simple solution, for UK businesses is to simply use in-house ''private clouds'' .Pearson highlighted that the current lack of transparency is preventing many users from reaping the true benefits of the cloud .For Identity and access management in the SaaS, has issued an Identity and Access Management

Guidance which provides a list of recommended best practices to assure identities and secure access management. Resource Locality and Data Segregation are the two key security challenges on which not much information is available in the existing literature, which necessitates that this can be further taken up for research.

4 CONCLUSION

There are numerous though advantages in using a cloud-based system, there are yet many practical issues which have to be sorted. Cloud computing is a disruptive technology with profound implications not only for Internet services but also for the IT sector as a whole. Still, several outstanding issues exist, particularly related to service-level agreements (SLA), security and privacy, and power efficiency. As described in the paper, currently security has lot of loose ends which scares away several potential users. Until a proper security module is not in place, potential users will not be able to leverage the true benefits of this technology. This security module should cater to all the issues arising from all directions of the cloud. Every element in the cloud should be analyzed at both the macro and micro level and subsequently an integrated solution must be designed and deployed in the cloud to attract and retain the potential consumers. Until then, cloud environment will remain cloudy. In a cloud, where there are heterogeneous systems having a variation in their asset value, a single security system would be too costly for certain applications and if there is less security then the vulnerability factor of some applications like financial and military applications will shoot up. On the other side, if the cloud has a common security methodology in place, it will be a high value asset target for hackers because of the fact that hacking the security system will make the entire cloud vulnerable to attack. In this paper an overview of cloud computing service delivery model, SaaS along with the security challenges , including both the traditional and cloud specific security challenges ,associated with the model has been presented A number of new challenges that is inherently connected to the new cloud paradigm has also been deliberated in the paper. As secure data storage in cloud environment is a significant concern which prevents many users from using the cloud, a practical solution to provide security and privacy for user data, when it is located in a public cloud, was also discussed in this paper. The need for further work on various security mechanisms has also been highlighted, in order to provide transparent services that can be trusted by all users.

References

[1] Heiser J. (2009) what you need to know about cloud computing security and compliance, Gartner, Research, ID Number: G00168345.

[2] Seccombe A.., Hutton A, Meisel A, Windel A, Mohammed A, Licciardi A, (2009). Security guidance for critical areas of focus in cloud computing, v2.1. Cloud Security Alliance, 25 p.

[3] Mell P, Grance T (2011) The NIST definition of Cloud Computing. NIST, Special Publication 800– 145, Gaithersburg, MD

[4] Choudhary V. (2007). Software as a service: implications for investment in software development. In: International conference on system sciences, 2007, p. 209.

[5] Pratap Murukutla, K.C. Shet (2012).Single Sign On for Cloud .In: International Conference on Computing Sciences, 2012IEEE DOI 10.1109/ICCS.2012.66

[6] Amlan Jyoti Choudhury, Pardeep Kumar,Mangal Sain, Hyotaek Lim, Hoon Jae-Lee(2011).A Strong User Authentication Framework for Cloud Computing. In: IEEE Asia -Pacific Services Computing Conference, 2011 IEEE DOI 10.1109/APSCC.2011.14 [7] Amazon Web Services: Overview of Security Processes http://aws.amazon.com/security Accessed: [January2013]

[8] Amazon. Amazon Elastic Compute Cloud (EC2). <http://aws.amazon.com/ec2/>. Accessed: [December, 2012]

[9] Cloud Security Alliance. Security best practices for cloud computing, 2010b<http://www.cloudsecurityalliance.org> [Accessed: July 2012].

[10] Cloud Security Alliance (2012) SecaaS implementation guidance, category 1: identity and Access management. Available: https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_Guidance.pdf

[11] Secunia. Xen multiple vulnerabilities; 2011. <http://secunia.com/advisories/26986/> [Accessed on 22 November 2012]

[12] Soft layer. Service Level Agreement and Master Service Agreement, 2009 /http: // www.softlayer.com/sla.htmlS [Accessed: October2012].

[13] European Union. Directive 95/46/EC of the European parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; 1995

[14] DTMF, 2013.Distributed Management Task Force. <http://www.dmtf.org/>. [Accessed: January 2013]

[15] SNIA. (2013).Storage Networking Industry Association. <http://www.snia.org/>. [Accessed: January 2013]

[16] OGF, 2010.Open Grid Forum, http://www.ogf.org/ [Accessed:August 2012]

[17] OCC, 2013. Open Cloud Consortium. <http://www.opencloudconsortium.org/>. [Accessed: January 2013]

[18] OASIS, 2013.Organization for the Advancement of Structured Information Standards. <http://www.oasis-open.org/>. [Accessed: January 2013] Cloud_Computing_Standards_Too_Many_Doing_Too_Little

[19] Kormann D, Rubin A. (2000) Risks of the passport single signon protocol. Computer Networks 2000; 33 (16): 51–8.

[20] Blaze M, Feigenbaum J, Ioannidis J, Keromytis AD. The role of trust management in distributed systems security, secure Internet programming, issues for mobile and distributed objects. Berlin: Springer-Verlag; 1999.p.185–210

[21] Cooper R. Verizon Business Data Breach security blog, 2008 /http://securityblog. verizonbusiness.com/2008/06/10/2008-data-breach-investigations-report/.