ISSN (e): 2250 – 3005 || Vol, 04 || Issue, 6 || June – 2014 ||
International Journal of Computational Engineering Research (IJCER)\

Software as a Service (SaaS): Security issues and Solutions

Navneet Singh Patel[1,] Prof. Rekha B.S.[2]
1 Dept. of ISE, R.V. College of Engineering, Bangalore, India
2 Assistant Professor, Dept. of ISE, R.V. College of Engineering, Bangalore, India

ABSTRACT:

Cloud computing is becoming increasingly popular in distributed computing environment. 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 disruptive technology is here to stay. Cloud computing can be seen as Internet-based computing, in which software, shared resources, and information are made available to devices on demand. But using a cloud computing paradigm 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, Privacy, Multi-tenant Architecture, Data Confidentiality, Service-level Agreements*

I. INTRODUCTION

A lot of studies and research has been done about Cloud Computing genre, by IT experts, business leaders and industry. While some believe it is a disruptive trend representing the next stage in the evolution of Internet, some believe it is just hype, as it uses earlier established computing technologies. 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 Seccombe [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). Adopting SaaS applications allow companies to save their information technology cost. The Cloud (or SaaS) model has no physical need for indirect distribution since it is not distributed physically and is deployed almost instantaneously. The customers do not take ownership of the software product, but instead they rent a total solution that is delivered remotely. The large majority of SaaS solutions are based on multi-tenant architecture. In this model, a single version of the application, with a unique single configuration (i.e. hardware, network, operating system), is used for every customers ("tenants"). But with its all attractive features there are a lot of issues that need to be identified and treated. Organization of this paper is as follows: Section 2 describes the related work and trends of Software as a Service (SaaS) delivery model. Section 3 lists some of misconception and reality about the SaaS. Section 4 describes the security issues that are posed by the SaaS. Section 5 lists some of the current solutions. Section 6 derives conclusion of the study done.

II. RELATED WORK AND TRENDS

According to a Gartner Group estimate, SaaS sales in 2010 reached $10 billion, and were projected to increase to $12.1bn in 2011, up 20.7% from 2010. Customer relationship management (CRM) continues to be the largest market for SaaS [4].

In an IEEE paper "A Privacy Preserving Repository for Securing Data across the Cloud" authors presented a privacy preserving repository for acceptance of integration requirements from clients to share data in the cloud and maintain their privacy, collect and integrate the appropriate data from data sharing services, and return the integration results to users [5].

A common approach to supply the data subject with information and control over data privacy is the provision of privacy policies specific to the data shared [6]. SLA negotiation is the subject of previous research based in the Gird community [7] and now extending into the cloud [8,9]. Within the cloud the SLA negotiation process involves the creation of a SLA captured using the WSAgreement XML standard [10].

In the cloud the service provider negotiates SLA on behalf of the user with cloud infrastructure providers. The process of an assessment of privacy has spurned a separate area of research in the form of Privacy Impact Assessments (PIA) [11]. PIA have emerged from existing work on data access by organisations in the 1920's to more specific mentions of PIA in terms of technology in the 1970s, a wide ranging study can be seen in [12].

As a result of widespread fragmentation in the SaaS provider space, there is an emerging trend towards the development of SaaS Integration Platforms (SIP). These SIPs allow subscribers to access multiple SaaS applications through a common platform. They also offer new application developers an opportunity to quickly develop and deploy new applications.

According to a survey of 600 enterprises by Enterprise Strategy Group 2012 indicate that SaaS use is bound to continue rising. In this survey 46% currently use it, 17% do not use but planning to use, 21% no use or plan but were interested to use, 14% no use, plan or interest and 1% was not clear [13].

Security is one of the most important concerns of SaaS. In a survey 51% of the people thought security the biggest concern where as 40% said integration with other application, 34% lack of customization and 33% total cost of ownership [14].

Fortunately, downward pressure on enterprise cloud providers to expose data security tools and options is beginning to have an effect. Newer companies are raising the competitive bar, providing first-generation tools to help customers see and control aspects of data security. HP has developed a program to assist enterprises in finding SaaS application vendors who are already taking an early lead in addressing the security injunction. HP Cloud Connections is a select affiliation of SaaS providers who have demonstrated best-of-breed customer security features.

III. MISCONCEPTION AND REALITY

The flexibility of cloud to scale bandwidth up or down at will, and its affordability as a pay-as-you-go service, have resulted in an interconnected, intelligent approach to smarter computing. The benefits of cloud computing are well-recognized. In fact, cloud computing ranks among the most popular new IT initiatives. Yet the excitement about cloud is often tempered by concern that this external delivery of services could compromise security. Cloud may seem new technology, but the fact is companies have been outsourcing their services and technology for many years. Service providers already deliver hosted technology offerings which are located offsite with client access using the Internet. And just because companies may give up some control to these service providers when they upgrade to a cloud-based environment (just like they give up some of their control in any outsourced arrangement), it doesn’t mean that they have to compromise on their security features.

Companies still weighing the advantages of cloud with the perceived security risk should begin by asking the right questions and examining the right considerations to help build a “trust and verify” relationship with the cloud provider that will support success. SaaS puts most of the responsibility for security management with the cloud provider and is commonly used for services such as customer relationship management and accounting. This popular option cloud is considered low-risk technology because it primarily deals only with only software and not with hardware or storage.

IV. SECURITY ISSUES

In Software as a Service (SaaS) model, the client needs to be dependent on the service provider for proper security measures of the system. The service provider must ensure that their multiple users don’t get to see each other’s private 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 [15]. Cloud computing providers need to provide some solution to solve the common security challenges that traditional communication systems face. At the same time, they also have to deal with other issues inherently introduced by the cloud computing paradigm itself.

A. Authentication and authorization

The authorization and authentication applications used in enterprise environments need to be changed, so that they can work with a safe cloud environment. Forensics tasks will become much more difficult since it will be very hard or maybe not possible for investigators may to access the system hardware physically.

B. *Data confidentiality*

Confidentiality may refer to the prevention of unintentional or intentional unauthorized disclosure or distribution of secured private information. Confidentiality is closely related to the areas of encryption, intellectual property rights, traffic analysis, covert channels, and inference in cloud system. Whenever a business, an individual, a government agency, or any other entity wants to shares information over cloud, confidentiality or privacy is a questions nay need to be asked

C. *Availability*

The availability ensures the reliable and timely access to cloud data or cloud computing resources by the appropriate personnel. The availability is one of the big concerns of cloud service providers, since if the cloud service is disrupted or compromised in any way; it affects large no. of customers than in the traditional model.

D. *Information Security*

In the SaaS model, the data of enterprise is stored outside of the enterprise boundary, which is at the SaaS vendor premises. Consequently, these SaaS vendor needs to adopt additional security features to ensure data security and prevent breaches due to security vulnerabilities in the application or by malicious employees. This will need the use of very strong encryption techniques for data security and highly competent authorization to control access private data.

.

E. *Data Access*

Data access issue is mainly related to security policies provided to the users while accessing the data. Organizations have their own security policies based on which each employee can have access to a particular set of data. These security policies must be adhered by the cloud to avoid intrusion of data by unauthorized users. The SaaS model must be flexible enough to incorporate the specific policies put forward by the organization.

F. *Network Security*

In a SaaS deployment model, highly sensitive information is obtained from the various enterprises, then processed by the SaaS application and stored at the SaaS vendor's premises. All data flow over the network has to be secured in order to prevent leakage of sensitive information.

G. *Data breaches*

Since data from various users and business organizations lie together in a cloud environment, breaching into this environment will potentially make the data of all the users vulnerable. Thus, the cloud becomes a high potential target.

H. *Identity management and sign-on process*

Identity management (IdM) or ID management is an area that deals with identifying individuals in a system and controlling the access to the resources in that system by placing restrictions on the established identities. Aria of IdM is considered as one of the biggest challenges in information security. When a SaaS provider want to know how to control who has access to what systems within the enterprise it becomes a lot more challenging task..

V. PROPOSED SOLUTIONS

There are several research works happening in the area of cloud security. Several organization and groups are now 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 [16]. 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 changes. The Cloud Standards website collects and coordinates information about cloud-related standards under development by the groups. The Open Grid Forum publishes documents to containing security and infrastructural specifications and information for grid computing developers and researchers.

We will discuss a security checklist for SaaS which can be used. To assess the security threats or capabilities of third-party SaaS providers, all customers need to ask some right questions:

A. *What metrics can be used for reporting?*

Will the service providers be able to present reports which will satisfy the CIO, the board and auditors that enterprise data is secured and meets regulatory requirements?

B. *What is the level of the access controls?*

The most established mechanism for data breaches now a day is through malicious or unintentional misuse of user access credentials. Visibility of the activity of individual users, which also includes administrative changes, is essential for data protection.

C. *Is provided data such that it can be easily adapted into internal monitoring tools, to preventing data silos?*

To make reporting simple and foolproof, you'll need to monitor enterprise's internal applications alongside SaaS applications, from a centralized dashboard.

D. How important and critical the enterprise data is?

Each SaaS application, must know the business criticality of the data involved. Is the SaaS application managing confidential customer data properly or not? You can then perform an inventory of the applicable compliance issues.

VI. CONCLUSION

Cloud computing is a disruptive technology with profound implications not only for Internet services but also for the IT sector as a whole. Though there are numerous advantages in using a cloud-based system, there are still many practical issues which have to be solved particularly related to privacy and security, service-level agreements (SLA), and power efficiency. As described in this paper, currently security has lot of issues 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. 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.

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]. McHall, Tom (7 July 2011). "Gartner Says Worldwide Software as a Service Revenue Is Forecast to Grow 21 Percent in 2011". Gartner.com. Gartner. Retrieved 28 July 2011.

[5]. Ranjita Mishra, Sanjit Kumar Dash, Debi Prasad Mishra, Animesh Tripathy "A Privacy Preserving Repository for Securing Data across the Cloud," Proc. Electronics Computer Technology (ICECT), 2011 3rd International Conference , pp. 6-10, 2011

[6]. J. Karat, C.-M. Karat, C. Brodie, and J. Feng. Privacy in information technology: Designing to enable privacy policy management in organizations. Int. Journal of Human-Computer Studies, 63(1-2):153–174 2005.

[7]. Hasselmeyer P, Qu C, Schubert L, Koller B, Wieder P. Towards autonomous brokered SLA negotiation. Proceedings of the 2006 eChallenges Conference—Exploiting the Knowledge Economy—Issues, Applications, Case Studies, Cunningham P, Cunningham M (eds.), vol. 3. IOS Press: Amsterdam, 2006

[8]. Rochwerger B, Galis A, Levy E, Caceres J, Breitgand D, Wolfsthal Y, IM Llorente MW, Montero R, Elmroth "E. RESERVOIR: Management technologies and requirements for next generation service oriented infrastructures." Proceedings of the 11th IFIP/IEEE International Symposium on Integrated Management, New York, U.S.A.,2009

[9]. Contract based e-Business System Engineering for Robust, Verifiable Cross-organisational Business Applications (CONTRACT), 2009

[10]. WS-Aggrement-Negotiation v 1.0 2011 http://www.gridforum.org/Public_Comment_Docs/Documents/2011-03/WSAgreementNegotiation+v1.0.pdf

[11]. R. Clarke, Privacy Impact Assessments February 1998, http://www.anu.edu.au/people/Roger.Clarke/DV/PIA.html

[12]. R. Clarke. Privacy impact assessment: Its origins and development. Computer Law & Security Review, 25 (2009)

[13]. Keep SaaS secure from the start, http://h30458.www3.hp.com/us/us/discover-performance/security-leaders/2012/jun/enterprise-saas-security-issues--concerns--threats---risks---hp-.html

[14]. 5 problems with SaaS security, http://www.networkworld.com/news/2010/092710-software-as-service-security.html

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

[16]. Cloud Security Alliance. Guidance for identity & access management V2.1,2010a

[17]. http://www.cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf [Accessed: July 2012].