Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.15 – 21

RESEARCH ARTICLE

Security Issues in SaaS Delivery Model of Cloud Computing

Aized Amin Soofi[1], M. Irfan Khan[2], Ramzan Talib[3], Umer Sarwar[4]

[1,2,3,4] College of Computer Science and Information Studies, Government College University, Faisalabad, Pakistan

[1] aizedamin@yahoo.com, [2] softchannel2000@hotmail.com, [3] ramzan.talib@gcuf.edu.pk, [4] sarwaroner@gmail.com

Abstract— SaaS (Software as a service) is one of the main service provided by cloud computing it has a feature of multi tenancy that virtually provides the services on one by one basis but physically all user utilize the services at same time. It has received considerable attention in past few years and an increasing number of countries show their interest in the promotion of SaaS market. Although it has received significant attention but security issue is one of the major inhibitor in decreasing the growth of SaaS. Many organizations may still be hesitant to introduce SaaS mainly because of the trust and security concerns, they may observe more risks than benefits in introducing this service. In this study an attempt is made to discuss the security issues and their existing solutions in SaaS delivery model of cloud computing.

Keywords— cloud computing; Software as a Service; SaaS security

I. INTRODUCTION

Cloud computing is an emerging technology which recently has drawn significant attention from both industry and academia. It provides services over the internet, by using cloud computing user can utilize the online services of different software's instead of purchasing or installing them at their own computers.

The National Institute of Standards and Technology (NIST) has defined 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 [1]. Gartner

defines cloud computing as a style of computing in which elastic IT-enabled capabilities are delivered as a service by using Internet technologies [2].

According to NIST [1] and Seccombe [3], guidelines for cloud computing, it has four different deployment models; (a) private cloud, it may be owned, managed and operated by the organization, a third party or some combination of them. (b) Community cloud, it may be owned, managed and operated by one or more of the organizations in the community. (c) Public cloud, the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed and operated by business, academic, or government organization. (d) Hybrid cloud, the cloud infrastructure is composition of two or more distinct cloud infrastructures. There are three different delivery models that are utilized within a particular deployment model. These delivery models are; (a) SaaS (Software as a Service), it enables the user to access online applications and software that are hosted by the service providers. (b) PaaS (Platform as a Service), it provides platform for developing applications by using different programming languages(c)IaaS (Infrastructure as a Service), provides the use of virtual computer infrastructure environment, online storage, hardware, servers and networking components

Fig1: NIST cloud definition Frame work [4]

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 considerable 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.

The global SaaS market is expected to reach 12.1 billion USD by 2014, reflecting a compound annual growth rate of 26%. This rapid growth of the SaaS market has had considerable influence on the software market [5, 6]. SaaS is an outsourcing innovation that transforms IT resources into continuously provided services [7]. This unique feature of SaaS has allowed the SaaS market to grow six times faster than the packaged software market and is expected to facilitate further development of SaaS [8]. However, despite of rapid growth of SaaS, it suffers with lot of security concerns. According to [5] new SaaS market, inducing SaaS adoption is likely to be difficult due to major inhibitors, such as limited integration and flexibility.

Our main area of concern in this paper is to highlight security issues and their existing solutions in SaaS model. This best-known branch of cloud computing represents a delivery model in which applications are hosted and supervised in a service provider's datacenter. The paper illustrates the assorted security issues of cloud computing with respect to SaaS service delivery model.

II. SECURITY ISSUES IN SaaS

Many vendors declared that adoption of SaaS technology can bring out many benefits to the users such as cost reduction, yet some organization are still not feeling comfortable in adoption of SaaS due mainly to trust concern e.g, data security [9,10]. The trust issue is needed to be improved to get the users attraction. SaaS is encouraging solution in expanding the organization's IT performance but many organizations still avoid in adoption of this technology because of lack of trust [11]. Most of the companies that have critical data wanted to self-support their own architecture or keep the data at their site or wanted to modify the software at their choosing but SaaS is not flexible to meet their needs.

The removal of data from service provider end is also a threatening issue. Hayes raises a point that there is no way to know that the cloud computing service providers properly deleted the client removed data or they saved it for some unknown reasons [12].In SaaS environment user do not know that where the data is exactly stores, cloud computing moves databases and application software's to large data centers where the management of services are not reliable. This sole aspect poses many new security challenges [13]. In SaaS environment 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 [14].

In the SaaS model, user data is stored at the SaaS provider's data center, along with the data of other users. If the SaaS provider is dealing with public cloud computing service, the enterprise data might be stored along with the data of other unrelated SaaS applications. The cloud provider might, additionally, replicate the data at multiple locations across countries for the purposes of maintaining high availability. There is a great deal of anxiety with the lack of control and awareness of how user's data is stored and secured in the SaaS model.

The key security rudiments should be carefully considered as a fundamental part of the SaaS application development and deployment process include; Data security, Network security, Data locality, Data integrity, Data segregation, Data access, Authentication and authorization, Data confidentiality, Web application security, Data breaches, Virtualization, Availability, Backup and Identity management [10]. Fig 2 indicates some important security issues in SaaS delivery model. Some of the important security challenges are described below.

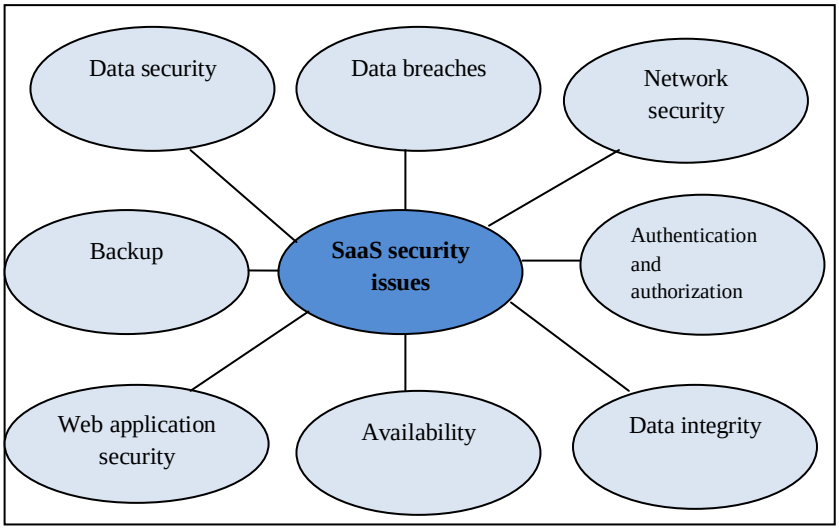

Fig 2: Security issues in SaaS

2.1 Data Security

Data security is one of the leading and most cited issue in SaaS delivery model. Data security may be a major concern for users who wants to introduce cloud computing. This technology needs proper security principles and mechanisms to eliminate users concerns. For example, most cloud services users have concerns about their private data that it may be used for other purposes or sent to other cloud service providers [15]. The user data that need to be protected includes four parts which are: (i) usage data; information collected from computer devices (ii) sensitive information; information on health, bank account etc. (iii) Personally identifiable information; information that could be used to identify the individual (iv) Unique device identities; information that might be uniquely traceable e.g. IP addresses, unique hardware identities etc.

2.2 Availability

The availability ensures the reliable and timely access to cloud data or cloud computing resources by the appropriate personnel. The SaaS application providers are required to make sure that the systems are running as it should be when needed and enterprises are provided with services almost all the time. This involves making architectural changes at the application and infrastructural levels to add scalability and high availability. Resiliency to hardware/software malfunction, as well as to defiance of service attacks, needs to be built from the ground up within the application.

2.3 Authentication 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. Lio introduces two factor password authentication scheme based on having both the properties of discrete logarithm problem and secure one-way hash function [16]. There were some deficiencies in Lio [16] work; to overcome those deficiencies Yang [17] introduce a mutual authentication scheme based on smart card and password. In which smart card user registers at the server firstly then chooses a right client to login and sends access request messages to the server. Then the server will complete mutual authentication with the user after receiving the messages.

2.4 Network Security

In a SaaS deployment model, susceptible data is obtained from the enterprises, processed by the SaaS application and stores at the SaaS vendor end. All data flow across the network needs to be protected in order to avoid outflow of perceptive 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 IP spoofing, port scanning, packet sniffing, etc. For highest protection, Amazon S3 is reachable via SSL encrypted endpoints. The encrypted end points are reachable from both the Internet and from within AmazonEC2, making it sure that data is transferred securely both within AWS and from sources outside of AWS [18]. However, malevolent users can exploit weak point in network security configuration to sniff network packets.

2.5 Backup

The SaaS vendor needs to ensure that all receptive enterprise data is backed up on regular basis to smooth the progress of quick recovery in case of devastation. Also the use of strong encryption method to keep the backup data is suggested to avoid unintended leaching of receptive information. In the case of cloud cloud service provider such as Amazon, the data at rest in S3 is not encrypted by default. The users need to independently encrypt their data and backups so that it cannot be accessed by unauthorized users.

2.6 Data breaches

Data from different users and organizations lie together in a cloud environment. The chance of breaching into the cloud surroundings will potentially attack the data of all the users. Thus, the cloud becomes a high value intention [19]. 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 [20]. Though SaaS supporter claim that SaaS providers can provide better security to customers data than by conventional means, Insiders still have access to the data but it is just that they are accessing it in a different way. Insiders do not have direct access to databases, but it does not reduce the risk of insider breaches which can be a massive impact on the security.

2.7 Data Integrity

Data integrity is one of the most serious elements in any system. Data integrity is easily achieved in an individual system with a single database. Data integrity in such a system is maintained via database transactions. Transactions should follow ACID (atomicity, consistency, isolation and durability) properties to ensure data integrity. Most databases support ACID transactions and can defend data integrity.
In a distributed system environment, there are multiple databases and applications. 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. One method for verifying the integrity of a set of data is based on hash values. A hash value is derived by condensing a set of data into a single unique value by way of a pre-defined algorithm.

2.8 Web application security

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 software product or building and deploying a new SaaS solution. One of the mandatory requirements for SaaS applications is that it has to be used and managed over the web [21]. Security gap in the web applications thus create a weakness to the SaaS application. In this scenario, the weakness can potentially have unfavorable impact on all of the customers using the cloud. Web applications introduce new security risks that cannot effectively be defended against at the network level, and do require application level defenses. The Open Web Application Security Project [22] has provided the ten most critical web applications security threats.

III. EXISTING SECURITY SOLUTIONS

Many researchers contribute their efforts to resolve the security threats like data security, network security, availability, backup and recovery, authentication etc., in this delivery model. Shutting down the unused services keep patches update and reduces accessibility of unknown users [23]. Security of data during processing may be possible by resource isolation which enables the deployment of VMs with isolation enhanced SLAs (service level agreement) [24]. In [25] technique provides a new way to authenticate in 3-dimensional approaches. It provides availability of data by overcoming many existing problem like denial of services and data leakage etc. But in this model, the data stored is not in encrypted form and once the login information is lost, the data can easily be retrieved by any unauthorized user.

In [26] kamara and lauter proposed a model by using technique that purely based on cryptographic storage services. In which when a user wants to send data to other user, they first generate a master key that encrypts their message. The message will be decrypted by the secret key for decryption stored on receiver system. The searching method is not very efficient for encrypted data. They discussed encrypted data searching techniques; symmetric searchable encryption (SSE) and asymmetric searchable encryption (ASE) but these techniques increase the complexity. [27] Discussed the drawbacks of symmetric searchable encryption (SSE) and asymmetric searchable encryption (ASE) techniques and suggested that these techniques are not useful over cloud. It introduce new model by using order preserving symmetric encryption (OPSE) technique but this model did not provide any information about the security attacks, confidentiality and integrity.

[28] Presents Cloud Proof, a secure storage system for increasing security over cloud. The proposed model use cryptographic tools to obtain an efficient and scalable system which allow users to detect and prove cloud misbehavior. This model helps users to detect

violations of confidentiality and integrity. [29] Proposed a three-layer system structure model in which each layer performs its own duty to ensure that the data security. First layer is responsible for authentication, Second layer is responsible for data encryption and third layer is for data recovery. [30] Discuss the problems in cloud computing like security of data, files system and backups and proposed a concept of digital signature with RSA algorithm, to encrypt the data while transferring it over the network. This technique solves the problem of authentication and security.

[31] Implement software to cloud provider. This software is implemented with two factor authentications and compares between eight modem encryption algorithms. The proposed software gets the faster and the highest security algorithm based on cloud infrastructure and it also advices to cloud users to select the most secure and faster algorithm that suitable to existing cloud architecture. [32] declares the data security is one of the primary inhibitor of cloud computing and provide analysis on data security across all stages of data life cycle and proposed a system to protect data using various schemes like airavat etc. This system can prevent privacy leakage without authorizations in map reduce computing process, the weakness in this work is that it was just a theory which depend on others schemes for its implementation.

The best security solution for web applications is to develop a development framework that has tough security architecture. In [33] four-tier framework for web-based development is proposed that though seems interesting, only implies a security facet in the process.

IV. CONCLUSION

In this paper an overview of cloud computing deployment and delivery models has been provided. As described in the paper there are many advantages of adopting SaaS delivery model of cloud computing such as reduction of operation cost and IT load etc. On the other hand there are yet many security concerns in this delivery model that needs serious attention of researchers to get the attraction of users. Although it is a fastest growing service of cloud computing but it suffers with security issues. A few studies are available in literature which addresses the different solutions of security problems but these solutions are not enough to fulfill the requirements of users. We also described some important security issues in SaaS model and their available solutions. Proper security measures are required to get the trust of users in this latest technology. Therefore security issues still need an exploratory study to revisit the dimensions of this research area. Data security is one of the major inhibitor in the growth of this well known technology. In future we are aiming to provide a detail systematic literature review on data security issue in cloud computing environment.

REFERENCES

[1] NIST SP 800-145, "A NIST definition of cloud computing", [online] 2012, http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf (Accessed: 23 December 2013).
[2] Gartner,"What you need to know about cloud computing security and compliance" (Heiser J), [online] 2009, https://www.gartner.com/doc/1071415/need-know-cloud-computing Security (Accessed 23 December 2013).
[3] 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.
[4] Mell Peter and Grance Tim, "Effectively and securely using the cloud computing paradigm"[online] 2011, http://csrc.nist.gov/groups/SNS/cloud-computing/cloudcomputing v26.ppt (Accessed 18 August 2013).
[5] Gartner "SaaS revenue is on pace to reach $12.1 billion in 2011" [online] 2009, http://www.channelworld.in/news/gartner-saas-revenue-pace-reach-121-billion-2011 126622011. (Accessed 10 December 2013) [Online].
[6] IDC "IDC: SaaS spending racing ahead" [online] 2010, http://www.computerworlduk.com/news/cloud-computing/3244663/idc-saas-spending-racing-ahead/.(Accessed 10 December 2013)
[7] Susarla, *et al*.,"Multitask agency, modular architecture, and task disaggregation in SaaS" in *Journal of Management Information Systems*, vol. 26, pp.87–118, 2010.
[8] IDC "IDC forecasts the software-as-a-service market to grow 6 times stronger than the overall packaged software market growth

in Asia/Pacific (excluding Japan) region" [online] 2009,. http://www.idc.com/AP/pressrelease.jsp?containerId=prHK21890709. (Accessed 1 December 2013).
[9] European Network and Information Security Agency (ENISA)"Benefits, risks and recommendations for information security"[online] http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing- risk-assessment. (Accessed: 28.December 2013).
[10] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, pp. 1-11, 2011.
[11] W.-W. Wu, *et al.*, "Exploring decisive factors affecting an organization's SaaS adoption: A case study," *International Journal of Information Management*, vol. 31, pp. 556-563, 2011.
[12] Hayes B. Cloud computing. Commun ACM 2008:9–11.
[13] Cong, *et al.*, "Ensuring data storage security in Cloud Computing," in *Quality of Service,2009. IWQoS. 17th International Workshop on*, 2009, pp. 1-9.
[14] V. Choudhary, "Software as a Service: Implications for Investment in Software Development," in *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, 2007, pp. 209a-209a.
[15] T. Elahi and S. Pearson, "Privacy Assurance: Bridging the Gap Between Preference and Practice," in *Trust, Privacy and Security in Digital Business*. vol. 4657, C. Lambrinoudakis, *et al.*, Eds., ed: Springer Berlin Heidelberg, 2007, pp. 65-74.
[16] I. E. Liao, et al., "A password authentication scheme over insecure networks , in " *Journal of Computer and System Sciences*, vol. 72, pp. 727-740, 2006.
[17] G. Yang, *et al.*, "Two-factor mutual authentication based on smart cards and passwords," in *Journal of Computer and System Sciences*, vol. 74, pp. 1160-1172, 2008.
[18] Amazon. "Amazon Elastic Compute Cloud (EC2)" [0nline] 2010, http://www.amazon.com/ec2/S (Accessed: 20 November 2013).
[19] Bernard Golden. "Defining private clouds," [online] 2009, http://www.cio.com/article/492695/Defining_Private_Clouds_Part_One (Accessed: 11November 2013).
[20] Cooper "Verizon Business Data Breach security blog" [online] 2008, /http://securityblog.verizonbusiness.com /2008/06/10/2008-data-breach-investigations-report/ (Accessed: 20 December 2013).
[21] Zalewski "Browsers security handbook"[onilne] 2009, /http://code.google.com/p/browsersec/S. (Accessed 20 December 2013)
[22] Bernard Golden. "Defining private clouds," [online] 2009, http://www.cio.com/article/492695/Defining_Private_Clouds_Part_Two (Accessed: 11November 2013).
[23] C. Kr, *et al.*, "Service specific anomaly detection for network intrusion detection," presented at the Proceedings of the 2002 ACM symposium on Applied computing, Madrid, Spain, 2002.
[24] H. Raj, *et al.*, "Resource management for isolation enhanced cloud services," presented at the Proceedings of the 2009 ACM workshop on Cloud computing security, Chicago, Illinois, USA, 2009.
[25] P. Prasad, *et al.*, "3 dimensional security in cloud computing," in *Computer Research and Development (ICCRD), 2011 3rd International Conference on*, 2011, pp. 198-201.
[26] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," in *Financial Cryptography and Data Security*. vol. 6054, R. Sion, *et al.*, Eds., ed: Springer Berlin Heidelberg, 2010, pp. 136-149.
[27] W. Cong, *et al.*, "Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 23, pp. 1467-1479, 2012.
[28] R. A. Popa, *et al.*, "Enabling security in cloud storage SLAs with CloudProof," presented at the Proceedings of the 2011 USENIX conference on USENIX annual technical conference, Portland, OR, 2011.
[29] D.Yuefa, *et al.*, Wu "DataSecurity Model for Cloud Computing" presented at *International Workshop on Information Security and Application* (IWISA 2009) Qingdao, China,November 21-22,2009.
[30] U. Somani, *et al.*, "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing," in *Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on*, 2010, pp. 211-216.
[31] E. M. Mohamed, *et al.*, "Enhanced data security model for cloud computing," in *Informatics and Systems (INFOS), 2012 8th International Conference on*, 2012, pp. CC-12-CC-17.
[32] C. Deyan and Z. Hong, "Data Security and Privacy Protection Issues in Cloud Computing," in *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, 2012, pp. 647-651.
[33] Tsai W, Jin Z, Bai X. Internetware computing: issues and perspective. In: Proceedings of the first Asia-Pacific symposium on Internetware. Beijing, China: ACM; 2009. p. 1–10.

