Exploration of Security Parameters to Evaluate SaaS

Ankit Banka, Anshul Saravgi
Department of Computer Science
Vellore Institute of Technology
Chennai, Tamil Nadu India
ankitbanka17@gmail.com,anshul.saravgi2010@vit.ac.in

Mangal Sain, Hoon Jae Lee
Department of Information Engineering
Dongseo University
Busan, South Korea
mangalsain1@gmail.com,hjlee@dongseo.ac.kr

Abstract— **In this modern era, cloud computing has evolved as a new technology for enterprise and personal computing. Many cloud services are available for customers in the market today. Each service has different terminologies, security, cost and goals. Evaluations of these cloud services are becoming more and more significant. Among the different types of cloud services available, SaaS is rapidly becoming a common software delivery model for many business applications, DBMS software, Management software, Virtualization etc. though users deploy Saas for different purposes, they are not aware about which one is suitable for them in terms of security, performance and storage capacity. The data privacy and service availability in cloud computing are major security problems. This paper proposes a system that addresses security challenges in context to SaaS. The development of such system will help users to judge different cloud computing services (SaaS) with respect to security issues, concerns and challenges of security in the cloud. On the other hand, vendors will able to identify the level of their service based on security parameters and basic requirements of SaaS. Customers will also be able to choose an appropriate SaaS provider for them, after evaluating the services based on parameters explored in the paper.**

Keywords— Cloud Computing, Cloud Services, Evaluation, Security, Service, SaaS

I. Introduction

Cloud computing is one of the most emerging technology with the rapid development of computer hardware and software. It provides more flexibility and availability at lower cost. Cloud computing helps users to get access to their resources via internet, dynamically from anywhere. Some of the corporations providing cloud computing platforms are Google, Amazon, IBM, Microsoft and VMware. Cloud computing services are delivered as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), to the users to provide all kinds of services on-demand to users. IaaS provides access to the computing resources in a virtualized environment over the cloud across a public connection (usually through internet). PaaS provides a platform and environment to allow developers to build applications and services over the internet. SaaS describes any cloud service where consumers are able to access software applications over the internet.

Traditionally, for any software requirement people used to buy the relevant software and then installed it on their computer to make use of it. Organizations also used to buy the software and then install the software on their network to utilize it. This led to the overhead of cost to establish infrastructure, maintenance, support and update. To overcome this, the concept of Software as a Service (SaaS) emerged out. As given in Buxmann et al. [1] SaaS can be defined as a "business or delivery model where software applications are accessible over the Internet and offered as on demand subscription". It is because of SaaS, that users are not bound to pay for the license, updates and maintenance for the software bought, which is advantageous for the customer.

With the increasing technology, businesses are moving steadily to the idea of paying a monthly subscription for software as a service. Because SaaS eliminates the high upfront cost, maintenance and support, organizations and normal users are taking the most advantage of it [2]. Necessary infrastructure is required to run the system which is shared across multiple clients. This lowers the cost of ownership per client. In the SaaS model, the data is stored at the SaaS service provider's data center, where other's user data also stored. Moreover, if the SaaS providers are leveraging a public cloud computing service, user data might be stored along with some other data which is not related to SaaS. The cloud service provider might also duplicate the data at various locations across different countries for the purposes of maintaining high availability. Hence, in the adoption of SaaS, the major concern for reluctance is the challenge of security [3], [4]. Security in SaaS is a very important and critical factor, which has to be addressed with its evolvement.

With the advancement of technology and the increasing number of SaaS service providers for different services, it is very difficult to evaluate them. There are several parameters related to SaaS which are unknown to normal as well as professional users. This paper addresses those parameters (related to security), based on which a SaaS service can be evaluated and ranked better in terms of security. With the help of this paper, users can know about all the security methods adopted by the SaaS providers and will be able to distinguish between different SaaS service providers based on security.

II. RELATED WORK

Li et al., worked on IaaS and PaaS only, to build the metrics for evaluating cloud services [5]. Collected metrics were based mainly on three aspects- Performance, Economics and Security. With respect to each, different evaluation metrics were identified. To design all such metrics, SaaS was not considered for evaluation. Security metrics identified were limited and brief. So there is need to explore the security metrics for proper evaluation in SaaS.

Some security challenges and vulnerabilities with respect to SaaS were further discussed in Infosys [6]. The work explores SaaS security challenges and describes how security testing could meet such challenges. Also, a prototype for evaluating SaaS security was given. It described how software testing could be applied to evaluate SaaS.

III. EVALUATION PARAMETERS

Software as service evaluation parameters can be categorized into 6 parts i.e. SaaS Deployment model, Data security and Integrity, Regulatory compliance, Availability, Backup, Identity management and Sign-on process. All the above mentioned categories are quite important to evaluate cloud services. Now, we formally described each category with its metrics to evaluate.

A. SaaS Deployment Model

SaaS security level depends upon which type of deployment model is used by the vendors. Vendor can use public cloud for deployment or they can host the service by themselves only. SaaS security mainly depends on the security of the public cloud, which can either be dedicated or shared. To make the SaaS more secured, public cloud or self hosted cloud should be secured. While evaluating SaaS, its deployment type should be considered more secured.

Table I shows the evaluation metrics with respect to the deployment model. Security will depend on the hosting model i.e. shared or dedicated, and also on how much secured shared or dedicated servers are. A brief introduction of both shared and dedicated server is given below.

- Dedicated hosting is a type of internet service in which a client leases the entire server that is not shared with anyone else. Client has full control over the server. This type of hosting is considered as more secured as compared to shared hosting.
- Shared hosting is a type of internet service in which more than one application of different clients run on the same server. Each client has only limited control over the server. This type of hosting is prone to more attacks and vulnerabilities.

TABLE I. DEPLYOMENT MODEL METRICSs

Deployment model	**Metrics**
Public	Dedicated
	Shared
Private	Dedicated
	Shared

B. Data Security

In SaaS model, data of the enterprise or user are stored on the vendor side. Hence corporation or users should know about vendor’s policy of securing data, to avoid losing or leakage of data [7].There are several methods to secure the data, as mentioned in Table 2. Each method has its own importance and drawbacks. But while evaluating, each one of them should be considered.

1) Data Encryption: It refers to the mathematical calculations and algorithm that converts the plain text to cipher text, which is not readable by unauthorized users. There are several algorithm to encrypt the data.

- *Client Encryption:* Information is converted into cipher text at the end point before sending it on the network [8].
- *Network encryption:* While moving the data from one end to the other end, there is high probability of data leakage due to man in the middle attack (MitM). Several techniques such as SSL, VPNs and TLS are therefore installed to perform network encryption of the data to avoid MitM.
- *Proxy Encryption:* It is a technique which allows a third party (proxies) to alter the cipher text which is encrypted for one party, so that it may be decrypted by other [9]. A cipher text under one key is transformed into another cipher text with different key by a proxy. However, proxy has no information about the original message [10]. Several applications such as distributed storage, email forwarding etc. are examples of proxy encryption.

2) Data Loss Prevention: There are several systems or software that detect potential data breach and prevent them by monitoring, detecting and blocking the sensitive data, whether they are at end points in the network or in the database [10].

- *Network Based:* Network based data prevention solutions are aimed at protecting the data while it is in motion. These types of prevention systems are installed at the perimeter of networks. They monitor network traffic to detect sensitive data that is being leaked out. This type of system can investigate email traffic, instant messaging, web 2.0 applications etc.

TABLE II. DATA LOSS PREVENTION

Data Encryption	Client Encryption	Network Encryption	Proxy Encryption
Data Loss Prevention	Network Based	Storage Based	End Point Based

- *Storage Based:* These types of systems protect the data in rest, i.e. data that resides in an enterprise database server.

- *End Point Based*: End-point based Data Loss Prevention (DLP) solutions focus on monitoring PC-based systems (laptops, tablets, POS, etc.) for all actions such as print or transfer to CD/DVD, webmail, social media, USB, and more. End-point based solutions are typically event driven. In such solution the agent resident on the end-point monitoring for specific user actions, such as sending an email, copying a file to a USB, leaking data or printing a file. These solutions can be configured for passive monitoring mode or actively blocking specific types of activities.

C. *Regulatory Compliance*

There is a need of periodical assessment of SaaS to meet regulatory and industry standards. Several regulations and standards are present to make the SaaS trustable. Standards such as SAS Type I and II are there to ensure physical and perimeter security of data centers and service providers. Also there are some regulations and standards such as ISO 27001, SOX, GLBA, HIPAA and PCI-DSS control which govern the access, storage and processing of sensitive data [11].

Table III lists all the regulatory compliance which is essential for SaaS providers to make their service trustable to the users.

SAS 70 Type I: SAS 70 is a worldwide recognized auditing standard which is developed by the American Institute of Certified Public Accountants [AICPA] in 1992. It confirms whether an organization have been through in-depth of all their control activities [12]. SAS 70 Type I audit includes controlled examinations that have been placed in operation. The audit also enquires about how its controls achieve the specified control objective for a stated period of time. Some of the key steps in SAS 70 audit process in shown in Figure 1. To perform a Type I audit it is a well-structured, multi-step process which includes various numbers of predefined processes and procedures, that must be completed to have a successful and in time completion [13]. This audit has used limited and is considered mainly for information purposes. It is not used as a basis to reduce the assessment of control risk below the maximum. For many years, many organizations successfully completed SAS 70 Type I standard and then move towards Type II compliance for long term value.

- *SAS 70 Type II:* SAS Type II audit includes controlled examinations that have been placed in operation and testing of operating effectiveness. In Type II audit, testing of controls are required with a minimum testing period of six months and cannot be more than twelve months. It may provide the user auditor with a basis for reducing assessment of control risk below maximum [14]. Internal and external effort is required. Third parties used to rely on these reports because verification is provided regarding these matters for a substantial period of time. Both SAS 70 Type I and II have been replaced by SSAE 16 in June 2011.

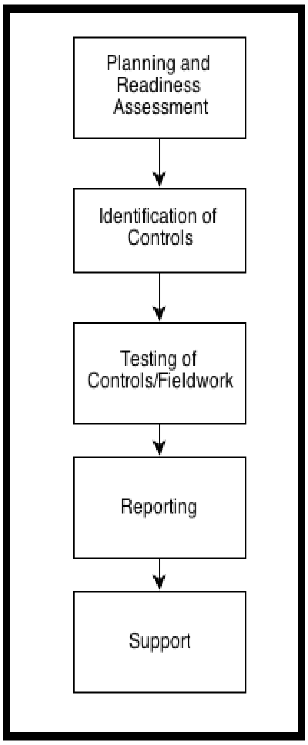
Planning and Readiness Assessment
Identification of Controls
Testing of Controls/Fieldwork
Reporting
Support

Fig. 1. Key Steps in SAS 70 Audit process

- *ISO 27001:* The ISO 27001 was published in October 2005. It is a specification for Information security management system. The objective of the standard is to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System" [15].With ISO 27001, service providers can show their commitment and compliance to global best practices, proving to customers that their security is superior to all others [16].

TABLE III. Regulatory Compliance

SAS 70	Type I	Type II
ISO 27001		
SOX		
HIPAA		
PCI-DSS		

- *SOX (Sarbanes-Oxley)*: It is a United States federal law that set new standards for all company

boards, management and public accounting firms [17].
The Sarbanes-Oxley act is arranged into eleven titles. Major elements of SOX are:

  - Public company Accounting Oversight Board.
  - Auditor Independence.
  - Corporate Responsibility.
  - Enhanced financial disclosures.
  - Analyst conflicts of Interest.
  - Commission resources and authority.
  - Studies and reports.
  - Corporate and criminal fraud accountability.
  - White Collar Crime penalty Enhancement.
  - Corporate Tax Returns.
  - Corporate Fraud Accountability.

- *HIPAA (Health Insurance Portability and Accounting Act):* It establishes national standards to protect people's electronic protected health information (PHI). HIPAA means that security of medical data is necessary for any vendor that deals with the medical information. Hence, the data center that stores such sensitive information should meet very strict standards to be HIPAA certified. Cloud service providers providing service to medical industry should certify their service with HIPAA to gain the trust of the client [18].
- *PCI-DSS:* In this modern era, payment cards such as credit card, debit card and stored value card plays an important role in online transaction. So their security concern is of high importance. There is a need of developing security standards which protect consumer data within the payment card industry [19]. "The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance card holder security and facilitate the broad adoption of consistent data security measures globally" [20].
  PCI DSS applies to all entities involved in payment card processing, which includes merchants, issuers, acquirers and service providers and also to the entities that process, store or transmit the card data. Below is the high level overview of the 12 PCI DSS requirements taken from [20].
  a) Install and maintain a firewall configuration to protect card holder data.
  b) Do not use vendor-supplied defaults for system passwords and other security parameters.
  c) Protect stored card holder data.
  d) Encrypt transmission of card holder data across open, public networks.
  e) Use and regularly update anti-virus software or programs.
  f) Develop and maintain secure systems and applications.
  g) Restrict access to card holder data by business need to know.
  h) Assign a unique ID to each person with computer access
  i) Restrict physical access to card holder data.
  f) Track and monitor all access to network resources and card holder data.
  g) Regularly test security systems and processes.
  h) Maintain a policy that addresses information security for all personnel.

D. Availability

The availability of service, offered by SaaS has become an important issue in selecting the most appropriate vendor. Without having a high availability level of the service provided by the cloud, advantages associated with cloud services are diminished.
Table IV shows several methods adopted by various cloud service providers to increase the level of availability.

  - *Data Redundancy:* Datacenters of various SaaS providers contains duplicate and useless data. This data should be cleaned up to increase the availability level of service. Cloud computing will be more efficient if data centers don't hold useless data.
  - *Transparency:* Cloud service providers should provide better transparency to their client. They should provide the information regarding availability to their customers.
  - *Cloud Optimization Services:* Another technique to improve the availability is to provide cloud optimization services. Using such service customers can customize the cloud services, such as level of availability, performance and security for each cloud component. This type of customization allows users to get the level of availability that is needed for a particular component. This technique increases the availability of several cloud components.

TABLE IV. Availability

Data Redundancy
Transparency
Cloud Optimization Services
SLA Agreement

  - *SLA Agreement:* Service Level Agreement (SLA) is a contract between the customer and the service provider about the level of service that will be provided to the customer. The SLA acts as a base for the level of service that will be provided by the SaaS vendors. Several parameters such as throughput, response time etc. are mentioned in SLA. Hence, before choosing a SaaS provider, customers should read SLA document properly to ensure quality of service provided by the vendor [21].

E. Backup

SaaS provider need to check that all the organization's important data is regularly backed up. They should make sure not to provide quick recovery in case of a disaster. Organizations should ensure that the SLA contains adequate guarantees regarding secure backup and recovery services. The requirement of strong encryption techniques is a must to prevent the sensitive information such as backed up data from accidental leakage.

For example in Amazon, the backup data at rest in S3 is not encrypted by default. Users need to encrypt their data separately and backup, so that it could not be accessed or tampered by any unauthorized source.

There are some assessments that test and validate the security of the data backup and recovery services provided by the SaaS provider. They include the following

- Insecure Storage
- Insecure configuration

If any vulnerability is detected during any of these tests, it can be exploited to gain access to sensitive enterprise data stored in backups.

F. Identity Management[IDM] and Sign-On Process

Within the cloud industry, identity management and sign-on process are considered high value, as they provide services for user-accounting processing, password management and secure authentication. Identity management has a simple purpose which ensures that user should be able to access only the data and applications they require, but it not as simple as it looks. The security challenges will differ depending upon which IDM and sign-on model is being used.

- *Independent IDM Stack:* The SaaS provider may also provide the complete stack of IDM and sign-on services. In such cases, the user account information and passwords are maintained at the SaaS provider's location and should be securely stored and processed. The SaaS provider should be able to support the strength and expiration policy of password of the organization to meet the regulatory demands.
- *Credential Synchronization:* The SAAS provider also used to provide support for user account information and credential replication between the organization and SaaS application i.e. the user account information is processed separately by each provider's customer within the customer's own boundary. Some user account information is replicated to the SaaS provider for authentication and authorization capabilities. The authentication occurs at the SaaS provider end using the replicated channels. The SaaS vendor needs to ensure the sanctity of these credentials and prevent their leakage.
- *Federated IDM:* The user account information including the credentials is managed and stored independently by each tenant. The authentication of the user will occur within the organization boundary. The identity of the user and some user attributes are propagated on demand to the SaaS provider using federation to allow sign on and access control.

Fig. 2 shows the Identity management methodology which includes the following steps:

a) *Inventory*: Current state analysis and evaluation
b) Create: Future state and gap analysis, build roles and identities required
c) Deploy: It maps privileges to roles, assign roles to workflows
d) Optimize: It adjust roles, workflows and identities as required
e) Report: Build reports for monitoring

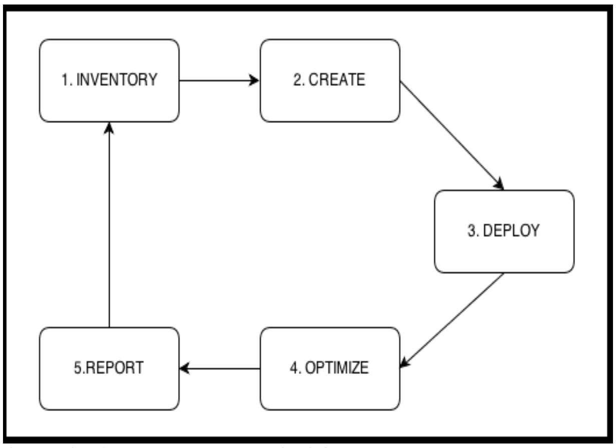

Fig. 2. Identity Management Methodology

IV. CONCLUSION AND FUTURE WORK

SaaS vendor offers different and various important services to the customers but, vendors should also address the issues and parameters related to security, performance and cost. This paper explores several parameters and fundamental requirements for a secure SaaS vendor. Vendors should provide all the information regarding the parameters discussed in this paper and should try to incorporate them in case they have not incorporated them till now. On the other hand, before selecting an appropriate SaaS vendor, customers should evaluate them based on all the parameters discussed in Section III. This paper tries to help both the customers and vendors to increase the level and quality of service provided by the SaaS.

Ranking the parameters based on certain criteria can be a future research to extend the evaluation level. With the help of these, an automatic system can be developed which will rank the SaaS providers based on ranking and weightage of each parameter. This type of system will surely be preferred by the customers and vendors.

After implementing such system vendors will be able to check whether their service is up to the level of requirement by the user or not and customers will be able to select the appropriate service for themself as per their requirements.

REFERENCES

[1] Buxmann, Peter, Thomas Hess, and Sonja Lehmann. "Software as a Service."*Wirtschaftsinformatik* 50.6 (2008): 500-503.

[2] Dubey, Abhijit, and Dilip Wagle. "Delivering software as a service." *The McKinsey Quarterly* 6 (2007): 1-12.

[3] Kandukuri, Balachandra Reddy, V. Ramakrishna Paturi, and Atanu Rakshit. "Cloud security issues." *Services Computing, 2009. SCC'09. IEEE International Conference on*. IEEE, 2009.

[4] Subashini, S., and V. Kavitha. "A survey on security issues in service delivery models of cloud computing." *Journal of Network and Computer Applications*34.1 (2011): 1-11.

[5] Li, Zheng, et al. "Building an Expert System for Evaluation of Commercial Cloud Services." *Cloud and Service Computing (CSC), 2012 International Conference on*. IEEE, 2012.

[6] Infosys:http://www.infosys.com/engineering-services/white-papers/Documents/SaaS-security-testing-cloud.pdf

[7] Popovic, Kresimir, and Zeljko Hocenski. "Cloud computing security issues and challenges." *MIPRO, 2010 proceedings of the 33rd international convention*. IEEE, 2010.

[8] Security guidance for critical of focus in cloud computing.
https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf

[9] Ateniese, Giuseppe, et al. "Improved proxy re-encryption schemes with applications to secure distributed storage." NDSS, 2005.

[10] Data Prevention
http://viewer.media.bitpipe.com/1240246133_118/1258558418_168/sCompliance_sSecurity_Data-Protection_final.pdf

[11] Rane, Pradnyesh. "Securing SaaS Applications: A Cloud Security Perspective for Application Providers." *Information Security Management Handbook* 5 (2010).

[12] Statement on Auditing Standards No. 70 http://www.worldcell.com/Files/definition-of-sas70.pdf

[13] What is SAS 70 Type I & II Audit Services? http://bmqr.org/what-is-sas-70-type-i-ii-audit-services-2/

[14] SAS 70 Services http://www.ecominfotech.biz/sas-70.php

[15] An Introduction To ISO 27001 http://www.27000.org/iso-27001.htm

[16] Getting Started with ISO/IEC 27001 Information Security Management http://www.bsigroup.com/en-GB/iso-27001-information-security/introduction-to-iso-27001/

[17] Piotroski, Joseph D. and Srinivasan, Suraj, Regulation and Bonding: The Sarbanes–Oxley Act and the Flow of International Listings(January 2008). Available at SSRN:http://ssrn.com/abstract=956987.

[18] Summary of HIPAA privacy rule http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/

[19] Morse, Edward A., and Vasant Raval. "PCI DSS: Payment card industry data security standards in context." *Computer Law & Security Review* 24.6 (2008): 540-554.

[20] Payment Card Industry(PCI) Data Security Standard https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

[21] Fawaz, Wissam, et al. "Service level agreement and provisioning in optical networks." *Communications Magazine, IEEE* 42.1 (2004): 36-43.

[22] Li, Zheng, Liam O'Brien, He Zhang, and Rainbow Cai. "On a catalogue of metrics for evaluating commercial cloud services." In *Proceedings of the 2012 ACM/IEEE 13th International Conference on Grid Computing*, pp. 164-173. IEEE Computer Society, 2012.

[23] Suresh, K. S., and K. V. Prasad. "Security Issues and Security Algorithms in Cloud Computing." *International Journal* 2, no. 10 (2012).