Software as a Service Security: Challenges and Solutions

Authors
Rajesh Kumar Mehta, Tanya Singh
Amity Institute of Information Technology, Amity University Uttar Pradesh, Noida, India
Email id-imrajeshraj@gmail.com, tsingh2@amity.edu

ABSTRACT
Cloud computing, without a doubt, has turned into the popular expression in the IT business today. Taking a gander at the potentials way it has on various business provisions and in our ordinary life. A large number of the peculiarities that make cloud system have tested the current security framework, as well as uncovered new security issues. This paper gives an analysis of the current status on cloud computing security issues focused around an itemized study conveyed by the author. It additionally makes an endeavour to depict the security challenges in Software as a Service model of cloud and also proposed a Security Model for SaaS(SMS) as a guide for assessing and enhancing security in each layer of SaaS delivery model

Keywords – cloud computing, SaaS security issue, SMS model

1. INTRODUCTION
Cloud computing is a cost-effective, reliable, secure and versatile delivery platform for providing IT Service over the internet. It is just a network of interconnected cloud system form a single big computing platform. Main objective of cloud computing system is to provide quick, secure, convenient data storage and online computing services with all computing features.

Cloud computing offers various advantage
-Computing Services are broadly accessible over the system and got to through standard technique that use by number of thick and thin client platforms like cellular phone, PDAs and Laptops.
-Cloud give real-time monitor resource utilization, balance the allotment of resources when required and it also deal with an assortment of diverse workloads, including the bunch of back-end operations and client turned intelligent provisions.
Cost productivity is the principle driver for cloud adoption. Other essential profits incorporate adaptability, deftness, scalability; better IT computing resources management and change management. As with any technology, cloud computing system has developed from being a guaranteeing business idea to one of the quickest developing fragments of the IT business. Presently companies are progressively understanding that essentially by tapping into the cloud they can increase quick get to best-of-breed business provisions or boost and save the infrastructure assets. But more information and data on people and organizations is set in the cloud system, concerns are starting to grow about how cloud safe and environment it is. Likewise with any innovation, however cloud raises numerous concerns including security, disaster recovery, administration and control, supplier management, enactments and regulations, and the absence of standards and rules. So as minimize the effect of these concerns and issues, risk mitigation in cloud is imperative if all organisations want to take the benefit and advantage of cloud system while ensuring and defending frameworks and information. To overcome issues in cloud and the implementation of controls are further complicated since measures and rules dealing with cloud security is very less.

The focus of this paper is to give recommended existing solution for the concern security issues at the SaaS level and also proposed layered security architecture for improved the scale of security. The rest of this paper is structured as follows: Section II is literature survey and in these section types of cloud, deployment models, security issues and survey. Section III explores cloud computing issue and also deal with service delivery model security issue and detailed focus on security issues on software as a service (SaaS) and also existing solution. Sections IV discuss the proposed model that will help in reduce security issues. Finally, in section V is conclusion.

2. Literature Review

The cloud computing system model has three service delivery models and four deployment model. For secure Cloud solution, an important choice is to pick the type of cloud deployment models. Presently there are mainly four models, which describe the where the cloud services and application can be used or installed. These are; a public cloud, private cloud, hybrid cloud model and community cloud. [1]

2.1 Public cloud

Public Cloud is model which allows consumer’s access to the cloud system via web browsers. It’s open for public and cost effective system for application hosting. [2] Example includes the Microsoft, Amazon AWS and Google. Public cloud model are less secure then the other deployment model because data accessed on the public system can be risky. There for privacy and trust issue are rife when we using services of public cloud.
2.3 Private cloud
Private Cloud is installed inside a private organization’s own data enter. This type of cloud is best for a single organization. It is less demanding to manage with security agrees ability and other concern administrative and provides more control over deployment cloud model. In the private organization deployment cloud infrastructure managed by the private firm or by a third part vendor and can be hosted externally or internally.

2.4 Hybrid Cloud
Hybrid cloud is a mix of public cloud, private clouds and community cloud. All clouds in the hybrid model are remaining distinct but is work together offering the advantage of multiple cloud deployment models. Hybrid deployment cloud model can also mean the feature of connect collocation, server management with cloud computing resources.

2.5 Community cloud
Community Cloud deployment model share infrastructure between many organization from a separate community with common security issue like jurisdiction, compliance and security. Whether these type of cloud is managed by a third party vendor or internally. Community cloud is used is best when in order to provide cloud solutions in them or security as well as the performance requirement.
To outline, in the cloud deployment model in the figure 1 we can see networking, storage, platform and programming base are given as administrations that may be all over relying on the consumer or user request. In choosing which deployment model to deploy, its depend upon the organization requirements.
In cloud computing, there are three service models

2.6 Infrastructure as a Service (IaaS).
IaaS Provides the client with the capability to storage, processing, network and other basic computing resources, and give the facility to consumer to send and run softwares, which can incorporate working operating system (os) and application. The user has control over os, deployed application, storage and limited control over networking components. IaaS also provides abstracted hardware, virtual machines and framework which may be controlled and oversaw through a service Application package interface. Example is Terre mark Enterprise Cloud, Rackspace Cloud, Amazon EC2. [3]

2.7 Platform as a Service (PaaS).
This layer works like Infrastructure as a service but it also gives additional level of functionality .like it provides the client with capability to deploy on the cloud computing infrastructure, client created application, developed using programming language and utility supported by the cloud provider. The platforms offered many other services like configuration management, development tools and deployment platforms or organization stages. Like Force, Microsoft Azure (MA) and Google AppEngine.

2.8 Software as a Service (SaaS)
SaaS is software or programming layer service offered by an outsider third-party or provider, accessible on interest through the internet or web and configurable remotely. It additionally works on the pay for every use costing and virtualized model where application is contracted by SaaS vendors. In this service all application has limited functionality it’s totally depending upon the pack is used or contracted. Example of Software as a Service is CRM service, online word processing (OWP), spreadsheet tools like Microsoft excel and web content delivery system services.

Figure 2: Cloud Service Delivery Model
Each one service model has distinctive implementations, as in figure 2, which muddle the advancement of security model for each one service delivery model in cloud computing. Virtualized resources, infrastructure as well as as virtual middleware stages and application provision are given and devoured as a service in the cloud computing environment. Cloud clients and vendors need to take care of cloud security framework at all levels.

3. SERVICE DELIVERY MODELS SECURITY ISSUES

We outline the security issues in all three service delivery model. Some of these problems are the obligation of cloud providers whereas others are the obligation of cloud customers.

3.1. IaaS Issues

IaaS delivery model comprises of a few parts that have been created through past years, in any case, utilizing those parts together in an imparted and outsourced environment conveys numerous difficulties. IaaS concentrates on overseeing virtual machines, in this danger are almost no not quite the same as with other cloud sorts here, the critical risk is maverick, rogue or baseless laying commandeering of services. Some security issues are VM Security, computer hardware security, hypervisor security and virtual network security.

3.2 PaaS Issues

The PaaS model ideal relies on the Service-oriented design (SOA) model. This ends up in receiving all protection setbacks that continue inside the SOA area such

<table>
<thead>
<tr>
<th>aggressions</th>
<th>Figure 3: Security Issues in SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mutual Authentication, DOS attacks, authorization, Replay attacks, as Man-in-the-middle attacks, WS-Security standards, cloud Injection attacks and input validation related aggressions are vital to safeguard the cloud endowed services. Above protection subject might be a public obligation amid cloud providers, customers and ability providers.</td>
<td></td>
</tr>
</tbody>
</table>

3.3 SaaS Issues

The SaaS Model consists of countless constituents that have been industrialized across past years; nevertheless, employing those constituents jointly in a public and outsourced environment carries several challenges. Protection and Privacy are the most momentous trials that could impede the Cloud Computing adoption. Breaching the protection of each component impact the supplementary components’ protection, subsequently, the security of the whole arrangement will collapse. In this section we study the protection
subject of every each component and discuss the proposed solutions and recommendations. [4]
In the SaaS model imposing and maintaining protection is a public obligation among the software vendors and cloud providers. The SaaS model inherits the protection setbacks debated in the preceding 2 models because it is crafted on top of every single of them encompassing data protection association (integrity, data locality, segregation, admission, backups, and confidentiality) and web security. Figure 1 Illustrate important security issues now I am focusing in detail on SaaS security issues. [4]

3.3.1 Application security
These provisions are normally conveyed by means that of the web through an internet program. Even so, defects in internet requisitions could create vulnerabilities for the SaaS provisions. Assaultants are utilizing the online to bargain clients' workstations and perform noxious exercises, for example, taking touchy data. Security challenges in SaaS requisitions aren't quite a similar as any web provision innovation; however accepted security results do not adequately guarantee it from strike, thus new methodologies are important. The Open web Application Security Project (OWASP) has recognized the 10 most discriminating internet requisition security dangers. There are a lot of security issues, however it's a great begin for securing internet requisitions.
3.3.2 Data Security
In cloud computing, chiefly openly cloud, users' data is stored and processed in cloud. Users cannot manipulation cloud groundwork, grasping their data that are the reason of menaces to the data. These protection setbacks considering users' data are displayed as bellow:

3.3.3 Data breach
It mostly violates 2 security properties of information: secrecy and trustworthiness. Privacy refers to just approved Parties or frameworks having the adaptability to get to the secured information. Integrity alludes to defensive keep protected from unapproved change and deletion. In a SaaS model the client's information is particularly keep and prepared at the SaaS vendor complete, so the information is at the possibility of break. The break conduct may hail from inside individual who works the information deliberately or coincidentally, or from outside malicious programmer. Therefore, the SaaS vendor should take measures to anticipate ruptures of the clients' information. There are a few answers for keep privacy, information trustworthiness, for example, fuzzy keyword look with low overheads, yet only for little scale cloud information usage framework. The result in will help secure evaluated quest for questions comprising of a solitary decisive word, whereas as the result in will help multi-keyword positioned inquiry over encoded cloud information, keeping low overhead on computation and communication

3.3.4 Data lock-in
It implies the client can't well move from a SaaS or IaaS vendor to an alternate. It may lose clients' information, which keeps clients from receiving distributed computing. Cog head is one sample of a cloud stage whose shutdown left clients scrambling to change their requisitions to run on an alternate stage. The standard result is to institutionalize cloud Application Programming Interface (API), case in point Go Grid API.

3.3.5 Data recovery
An episode like a server breakdown may cause harm or misfortune to clients' information. To beat this, information should be backed up to be recouped in future. Cloud clients will keep a reinforcement of crucial data on a neighbourhood machine. The SaaS vendor offer gives reinforcement service for clients. Case in point, Amazon's S3 (Simple Storage Service) allows a client to define the records that ought to be backed up and also the standard level of data mirroring.
3.3.6 Multi-tenancy
The multi-tenancy feature stems from the virtualization layer and permits storing info from multiple customers at an equivalent physical hardware. This situation promotes attackers to take advantage of this configuration in the kind of co-location, co-residence, or co-tenancy attacks, whereby an assaulter is able to disguise as a regular and bonafide customer to infiltrate neighbour VMs belonging to different real legitimate clients. Several aftermaths are possible, as well as compromising integrity, confidentiality and privacy. Hacking through loopholes or injecting consumer code into the SaaS model is 2 possible ways in which to attain that purpose. To tackle these problems, data should be segregated, that means that SaaS systems have to assure clear boundaries between customer’s data.

3.3.7 User Frontend
Besides the particular problems derived from insecure frameworks and platforms, other problems arise from the user frontend to services. In other words, because clouds give on-demand self-service capabilities, services signed by customers need management interface with fine-grained configurations of those services. Usually, those interfaces are accessible via the web, thus being at peril due to web related security problem. Moreover, there's probability likelihood of exploiting those administrative interfaces in clouds than in different systems where management Functionalities are only accessible to a few administrators.

3.3.8 Control
Control refers to regulating the use of a system composed of an infrastructure, data, applications and services. Whereas a customer may worry about malicious usage and malicious computation, a service provider is also worried regarding monitoring and logging events inside the cloud systems, because standards and control mechanisms are scarce. Log files record all tenant events. Thus, insufficient logging and monitoring capabilities might hamper or stop pruning for a single tenant.

3.3.9 Platforms and Frameworks
Given that clouds follow a SOA approach, the matter the problem integrity gets increased when compared to alternative distributed systems [95]. Moreover, net services ordinarily rely on extensible mark-up language (XML), SOAP and representational State Transfer (REST), and APIs. Most vendors deliver their apes without transactions support, that any complicates the management of information integrity across multiple
SaaS applications. Additionally, the PaaS model provides platform and frameworks to develop cloud applications. Throughout the applications development lifecycle, programmers should deploy rigorous security measures specializing in authentication, access control and encoding. However, unsafe APIs and ides (may allow hosting botnets and Trojan horses) with insecure systems calls or deficient memory isolation could comprise points of entrance to attackers

3.3.10 Resource Locality
In a Saas model of a cloud benefit, the end-customers use the administrations gave by the cloud suppliers without knowing decisively where the assets for such administration are placed, maybe in other definitive zones. This speaks to a possible issue when happen, which is as a less than dependable rule past the organization of cloud control. Because of consistence and data security laws in numerous nations, area of information is of most extreme important in much enterprise design plan. The European Union has issued a Directive 95/46/EC to shield the client security no matter what. The order precludes exchanges of individual data to nations which don't guarantee a sufficient level of insurance. As a case, the late Drop box clients need to consent to the "Terms of Service" that allow the suppliers the right to unveil client information in agreeability with laws and law authorization demands. Also to the issue of nearby laws and there's additionally the inquiry of under whose ward the data falls, once an examination happens. A protected SaaS model must be fit for giving best services to the customer on the area of the information of the client.

3.3.11 Network Issue
In a Saas sending model, sensitive information is gotten from the wanders, converted by the Saas requisition and keep at the Saas merchant end. All information stream over the framework must be secured with to stop spillage of data. This incorporates the usage of system framework movement encryption routines like Secure Socket Layer (SSL) and the Transport Layer Security (TLS) for security. On the off chance that there ought to be an event of Amazon web Services (AWS), the framework layer gives vital security Against routine framework security issues, in the same route as MITM (Man-In-The-Middle) attacks, IP ridiculing, port checking, pack sniffing, et cetera for perfect security, Amazon S3 is accessible through SSL mixed endpoints. The scrambled end focuses are open from every the net and from inside Amazonec2, ensuring that data is exchanged safely each among AWS and to and from sources outside of AWS. Nonetheless, malicious clients will misuse shortcomings in system security setup to sniff system packet.

4. CURRENT SECURITY SOLUTIONS
There are a few experimental works happening in the era of cloud security. A few gatherings and association are intrigued by creating security results and gauges for the cloud some of the security concern and their
solution is showed in Table 1. The Cloud Security Alliance (CSA) is solution suppliers, non- benefits and people to enter into exchange about the present and future best practices for data confirmation in the cloud. The Cloud Standards site gathers and directions data about cloud-related guideline being worked on by the peoples. The Open Web Application Security Project (OWASP) keeps up arrangement of top vulnerabilities to cloud-based or SaaS models which is overhauled as the danger scene changes. The Open Grid Forum distributes reports to holding Security and infrastructural determinations and data for matrix figuring designers and specialists. The best security answer for SaaS requisitions is to create an improvement Pattern that has compelling security structural arranging. Tsai W, set forward a four-level structure for web progression that however seems intriguing, simply construes a security offer simultaneously. In his work, Berre has proposed an aide towards cloud-driven progression, furthermore the X10 way is one of the methodologies to achieve better use of cloud capacities of immense parallel get ready and concurrency. an alternate philosophy is stake withdrawal to surety security of data all through planning, by withdrawing the processor saves in virtual machines, and isolating those virtual stores from the hypervisor store. One essential result, for UK associations is to fundamentally use in-house "private fogs" Pearson highlighted that the current Absence of transparency is keeping various customers from collecting the authentic benefits of the cloud.

**Table 1: Security Areas and solution in SaaS [5]**

<table>
<thead>
<tr>
<th>S.No</th>
<th>Security Areas</th>
<th>Possible Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Information Security</td>
<td>• Information Security Risk Management Framework</td>
</tr>
<tr>
<td>2</td>
<td>Cloud standards</td>
<td>• Cloud Security Alliance (CSA)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ITU Cloud Computing Focus Group</td>
</tr>
<tr>
<td>3</td>
<td>Data Access</td>
<td>• Multi-user access policies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Data Access Management</td>
</tr>
<tr>
<td>4</td>
<td>Web application security</td>
<td>• Web Application Scanners</td>
</tr>
<tr>
<td>5</td>
<td>Backup</td>
<td>• Agentless Method for data Backup and Recovery</td>
</tr>
<tr>
<td>6</td>
<td>Identity management and sign-on process</td>
<td>• CSA’s Identity and Access Management Guidance</td>
</tr>
<tr>
<td>7</td>
<td>Network Security</td>
<td>• Network Security for virtual machines</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Network Security Sandbox</td>
</tr>
<tr>
<td>8</td>
<td>Authentication and authorization</td>
<td>• Open Authorization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Two Factor Authentication</td>
</tr>
<tr>
<td>9</td>
<td>Availability</td>
<td>• Data Deposition</td>
</tr>
<tr>
<td>10</td>
<td>Data confidentiality</td>
<td>• Attribute based Proxy Re-Encryption</td>
</tr>
</tbody>
</table>

For Identity and access issue in the Saas has issued an Identity and Access Administration Guidance which gives a plan of proposed best practices to affirm character more secure access organization. Asset of cloud
Locality and Data Segregation are the two key security challenges on which almost no information is available in the ebb and flow composing, which obliges that this could be further devoured for examination.

5. PROPOSED SECURITY ARCHITECTURE

As a result of this research, we propose a Security Model For SaaS (SMS) as a guide for assessing and enhancing security in each layer of SaaS delivery model as shown in Fig. 3. SMS model consists of three sides, 1) Self Protective Identity Layer 2) User Access Control Layer and 3) Data Security layer. Now I am going to discuss each layer in detail.

![Diagram](image)

**Figure 4: Proposed Security Layered Architecture**

This figure shows that three layered security approach in cloud computing. Proposed layered architecture which solves the above mentioned security issues in cloud system.
5.1 Self Protective Layer
This is the first layer which manages the controls to the cloud services by detecting any feasible intrusions and deal with them. It can be divided into two sub-layers. One is network and another at application level. Network based IDS attempt to expose illegal entry to network by configuring the network traffic packets like UDP, TCP and IPX/SPX and analyze the contents against a collection of rules. NIDS is prepared up of a mix of uni-utility sensors and configured according to the policies and rules of the provider that are settled at dissimilar points within the network. As an example it can accept the packet and discard the packets according to the rules define by the cloud provider. The one is Application level intrusion detection system using the good authentication tool. It can handle like unauthorized access by malicious bots or user.

5.2 User Access Control Layer
User Access Control Layer is combination of 3 sub-layer.UACL manages the users according to the predefined roles and allocated privileges and allowed resources. The first layer check the user or consumer roll in the cloud system it ensures consumer cannot swap their roles .the second layer is responsible for verifies the privileges. The last layer mange the available resources according to their roles and privileges. This layer channels the clients on the premise of their Predefined roles and relegates them the benefits and Resources. The 3 sub-layers further include security as they Further guarantee that the client can't swap parts or any Gatecrasher can't get access to the assets. The principal of These layers verities the parts relegated to the client and Can even relegate default part to any new client. This layer Is likewise in charge of keeping note of any part Acceleration that has happened and can even rollback the Acceleration. The next level checks the benefits relegated to the client and verifies whether they match the role that the client has and any conflict could prompt repudiating of any extra benefits. The third sub layer deals with conceding the resources to the client focused around his roles and privileges.

5.3 Data Security Layer
Lowest layer in this model is data security layer (DSL). It comprises of mainly there sub-layer. DSL is responsible for data protection from deletion, accidental problem and prevention of illegal use of data. All sub-layer work together to maintain the security of data.DSL is governed by the rules set by the cloud computing system providers. The cloud data layer security is the least level of security that the cloud supplier can apply. This incorporates security of information from coincidental access or deletion and counteractive action of unapproved utilization of data the three sub layers can cooperate to guarantee security of the information. The layers are completely legislated by the strategies set by the cloud supplier. The first layer guarantees isolation of
information regardless i.e. regardless of the fact that the encryption tails at any stage this layer guarantees the isolation of information. Furthermore data encryption is a key some piece of putting away the information on cloud as the information is extremely defenceless against outside access. The information encryption utilized ought to be solid enough however in the meantime it ought to have the capacity to adapt with colossal volumes of information. This issue however has been countered, all things considered, by the Hard circles which encode any information that is put away on them and likewise By the accessibility of secure fittings which don't let the supplier get to the memory when information is, no doubt transformed. An alternate perspective is that of recovery, the suppliers must give a backup to all the information that the client has so if there should arise an occurrence of any accidental deletion the information could be effectively recovered

6. CONCLUSIONS
In spite of the fact that Cloud computing could be seen as another marvel which is situated to upset the way we utilize the Web, there is much to be wary about. There are numerous New innovations developing at a fast rate, each with New technology and with the capability of making Human’s lives simpler. However one must be extremely cautious to comprehend the limits and security dangers postured in using these innovations. So cloud system is not example of exception. In this paper key security contemplations and difficulties Which are at present confronted in the Cloud system are highlighted and discuss about the SaaS security issues and existing solution? The proposed solution is discussed in this paper that is secure model for SaaS (SMS0. In this model A decently characterized layered methodology is important to guarantee the security at every level. The model Exhibited here guarantees that every single part of the Web administration is secure and the trust inside the clients Might be created. The methodology might be effortlessly connected and changed according to the client requirements with available software. Cloud computing has the possibility to turn into a leader in, Secure virtual and financially reasonable IT service. Future work is more advancement in this technology and standard.

7. REFERENCES


[4] Mariana Carroll, Alta van der Merwe, Secure Cloud Computing, Metropolitan University, South Africa

