SECURITY ISSUES IN CLOUD COMPUTING: A REVIEW

Shishobitveer Singh Sohal
Department of Computer Science & Engineering
DAVIET, Jalandhar

Gursewak Singh
Department of Computer Science & Engineering
DAVIET, Jalandhar

Abstract—Network security has become one of the biggest uprising points of concern now days. People are getting attached more and more to the internet in order to fulfill their demands. Not only customers but also the IT based companies are also getting themselves relying on up growing technology called as cloud computing. Cloud is a branch of computer science that provides the services on lease. In this paper we will make a comparative analysis of various technical security issues towards cloud computing, cloud deployment based security and model based security issues. We will also make a tabular comparative analysis at the end of the paper.

Keywords— cloud computing, security issues, cloud models

1. INTRODUCTION

With the progression in the period the innovation is getting increasingly and more extensive. Individuals now a day's get the administrations as per their requests thusly they don't need to pay superfluous for the things they don't need to utilize. Cloud computing is one the developing innovation which give the administration of programming on rent. Cloud computing permits the client to make requests and give the administrations as need by the clients. Cloud computing is productive and adaptable however keeping up the steadiness of preparing such a variety of occupations in the cloud computing environment is an exceptionally complex issue with security of data to which is getting much consideration by the scientists [1]. Cloud computing as such is the moral story of the web [2]. The cloud specialist organizations should sure about that they get the security flanks appropriate, for they are the ones who will assumed the liability if things turn out badly. Cloud framework offers many advantages like quick sending, pay-for-utilize, lesser costs, adaptability, flexibility, universal system get to, more noteworthy versatility, hypervisor insurance against system assaults, ease recuperation and information stockpiling arrangements, on-request security controls, continuous identification of framework altering and fast re-constitution of administrations [3]. The real favorable position of cloud computing in which we can pay-for-use for any product i.e. on the off chance that a client doesn't have a specific programming that he needs to utilize say MS word, the client can utilize that specific programming on the cloud framework by paying for it. Cloud framework comprises of three administration models in light of the asset center [4] i.e. SaaS, PaaS and IaaS. Within this paper our key goal is to deliver an evolution and qualified study of various cloud computing security issues. First we will bounce an outline of all the security issues either model based or
deployment based. At the last we will conclude the paper in a tabular form.

2. TECHNICAL SECURITY ISSUES IN CLOUD COMPUTING

In this discussion, we present some security issues related to Cloud Computing. Each issue is explained briefly and tells how it makes an impact on the cloud system technology.

2.1 XML SIGNATURE ATTACK

There are numerous conventions that utilization the XML Signature for their verification and trustworthiness. To those conventions XML Signature assault is extremely normal and called as XML Signature Element Wrapping [5]. As this sort of assault applies on the web benefits so its clear that it is regular in the distributed computing as well. The underlying message shows a message sent by an honest to goodness customer. The body contains a demand for the document marked by the sender. The Signature is encased in the message header and alludes to the marked message. The message section utilizes an X Pointer to that contains the estimation of "body".

In the event that an aggressor spies such a message, he can play out the assault as took after. The first assemblage of message is moved to a crisply embedded wrapping component (giving the assault its name) inside the message header, and another body is made. This body contains the all operation the intruder needs to perform with the first sender's approval, here the demand for the specific record. The subsequent message will even now contain a substantial mark of an honest to goodness client. Since the first mark still exist in the message so the trespasser can without much of a stretch get to the data on the cloud thus can alter it.

2.2 BROWSER SECURITY

The fundamental component of Cloud computing is that it can be accessed from anywhere remotely. The customer PC utilized for verification and for I/O and that PC additionally charges to the cloud for the further operation. So clearly to access any framework or a system the browser is a key point. With concentrating on the Same Origin Policy (SOP) [6], this report unfurls numerous weaknesses of browser security in cloud framework. For this examination we need to consider TLS, which is utilized for host validation and encryption of information. The deficiencies in the Web browsers are that it can't straightforwardly make XML Signature or XML Encryption. As Data must be scrambled through TLS, and marks are just utilized as a part of the TLS handshake. In here the browser goes about as detached information stockpiling. Since the browser itself can't produce cryptographically legitimate XML tokens to verify against the Cloud, this is finished with the assistance of a trusted outsider. With the anatomies of scripting dialects (as JavaScript) into Web pages, it got to be distinctly essential to characterize get to rights for these scripts. So it's a characteristic thing, the browser with same cause, [7] permits the operations of read/compose operations and to forbid any entrance to content from an alternate starting point.

2.3 CLOUD MALWARE INJECTION ATTACK

Among the key assaults on the cloud framework the malware infusion assault is an extensive assault endeavor goes for infusing a noxious administration execution into the Cloud framework. Such sort of Cloud malware fills for a specific need. The motivation behind cloud malware is enemy that might run from listening in by means of moment information alteration to full usefulness changes or blockings. To make the enemy the malware needs to make its own
particular execution module (SaaS or PaaS) or virtual machine case (IaaS), and add it to the Cloud framework.

2.4 FLOODING ATTACKS
Outsourcing is a major aspect of Cloud Computing consists in basic operational tasks to a Cloud system provider. Among these basic tasks, maintenance of server hardware is the most important one. So instead of operating an own, internal data center, the paradigm of Cloud Computing enables companies (Users) to rent server hardware on demand (IaaS). This approach is economically beneficial when it comes to dynamics in server load, as for instance day-and-night cycles can be attenuated by having the data traffic of different time zones operated by the same servers. No doubt the feature of providing more computational power on demand is appreciated in the case of valid users but it poses severe troubles in the presence of an attacker. The corresponding threat that arises or may arise is flooding attacks, in which basically an attacker sending a large amount of meaningless requests to a certain service. As each of these requests has to be processed by the service implementation in order to determine its invalidity and due to this heavy load it causes a certain amount of workload per attack request, which creates flood of requests usually would cause a Denial of Service to the server hardware [8], [9]. In the specific case of Cloud Computing systems, the impact of such a flooding attack is expected to be amplified drastically. This is due to the different kinds of impact. Flooding of requests then further may lead to halt the running system and it makes easy to attack of denial of service. The denial of service is of two types direct and indirect [10].

3. CLOUD DEPLOYMENT BASED SECURITY
In the cloud deployment model, networking, platform, storage, and software infrastructure are delivered as facilities that gauge up or down conditional to the mandate. The Cloud Computing model has three main deployment models which are:

3.1 PRIVATE CLOUD
Private cloud is another term that a few merchants have used to depict offerings that copy cloud figuring on private systems. It is a set up inside an association's inward endeavor datacenter. In the private cloud, versatile assets and virtual applications gave by the cloud merchant are pooled together and accessible for cloud clients to share and utilize. It contrasts from general society cloud in that all the cloud assets and applications are overseen by the association itself, like Intranet usefulness. Usage on the private cloud can be much more secure than that of general society cloud in view of its predetermined inward introduction. Just the association and assigned partners may have entry to work on a particular Private cloud. [12]

3.2 PUBLIC CLOUD
Public cloud portrays cloud registering in the conventional standard sense, whereby assets are powerfully provisioned on a fine-grained, self-benefit premise over the Internet, through web applications/web administrations, from an off-webpage outsider supplier who offers assets and bills on a fine-grained utility figuring premise. It is ordinarily in view of a compensation for every utilization display, like a prepaid power metering framework which is sufficiently adaptable to provide food for spikes popular for cloud optimization. [13] Public clouds are less secure than the other cloud models since it places an extra weight of guaranteeing all applications and information got to on the public cloud are not subjected to malevolent assaults.

3.3 HYBRID CLOUD
Hybrid cloud is a private cloud connected to at least one outer cloud administrations, halfway oversaw,
provisioned as a solitary unit, and surrounded by a safe system [14]. It gives virtual IT arrangements through a blend of both open and private clouds. Hybrid Cloud gives more secure control of the information and applications and permits different gatherings to get to data over the Internet. It additionally has an open design that permits interfaces with other administration frameworks. Hybrid cloud can portray arrangement consolidating a nearby gadget, for example, a Plug PC with cloud administrations. It can likewise depict designs consolidating virtual and physical, arranged resources for the most part virtualized environment that requires physical servers, switches, or other equipment, for example, a system machine going about as a firewall or spam channel.

4. MODEL BASED SECURITY ISSUES
Cloud framework comprises of three conveyance models that characterize the structure of the cloud framework. Three models in cloud framework are SaaS, PassS and IaaS. SaaS remains for software as a service in which client can utilize the information from untouchable limits of any undertaking. PaaS remains for Platform as a service that gives the stage to building the applications on the cloud. The last one IaaS remains for infrastructure as a service which gives equipment support to cloud framework. In any case, these models additionally have some security openings that are examined as follows in the paper.

4.1 ISSUES IN SOFTWARE AS A SERVICE(SAAS) MODEL
The SaaS essentially accentuating on supplanting the old application programming with the new ones as opposed to making the convey ability of utilization programming in which the security usefulness of programming application is principle center [11]. The fundamental issue in SaaS is that the information is exceptionally delicate on the grounds that it is put away on the outside the limit of big business. For safety efforts the customer needs to rely on the supplier in SaaS. Because of perceivability of information of each other clients, the supplier must accomplish something so that the information robbery or misfortune is evaded. There is likewise another issue i.e. in the event that a specific client needs a similar document which is being utilized by another client in the meantime yet because of safety efforts the client can't get that record.

4.2 ISSUES IN PLATFORM AS A SERVICE(PAAS) MODEL
PaaS is more extensible than SaaS as it gives stage to build up the application yet security is the fundamental issue once more. At the point when PaaS gives individuals to manufacture their applications on the larger amount of stage, the supplier must guarantee about detachment of information between two applications.

4.3 ISSUES IN INFRASTRUCTURE AS A SERVICE(IAAS) MODEL
IaaS bargains in virtualization and VMware. Any issues emerge in VM May prompts to defer in conveyance of bundles in upper model like PaaS and SaaS. Additionally IaaS has higher security administration strategies and prompts to less security openings in it [12].

Table 1: comparative study of technical security issues in cloud computing
### Table 2: Comparative Study of Model Based Security Issues

<table>
<thead>
<tr>
<th>Security Issues</th>
<th>Attack Description</th>
<th>Effect on Cloud System</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td>XML Signature Attack</td>
<td>Addition of new body to novel message</td>
<td>Novel information altered</td>
<td>Usage of secure coding</td>
</tr>
<tr>
<td>Browser Security</td>
<td>Data is kept passively so browser is impotent to cause tokens of authentication</td>
<td>Data loss occurs</td>
<td>Use xml encryption in TLS</td>
</tr>
<tr>
<td>Malware Injection Attack</td>
<td>Malware makes its own enactmentunit and swell it to cloud system</td>
<td>May leads to malicious service operation and incorrect code performed</td>
<td>Store hash values on novel service instance's file and relate it with the hash value of file</td>
</tr>
<tr>
<td>Flooding</td>
<td>Performance of needless applications sent by intruder</td>
<td>Full harm of availability to envisioned services</td>
<td>Allow only authenticated service to execute and use scheduling</td>
</tr>
</tbody>
</table>

### Table 3: Comparative analysis of Cloud Computing Challenges

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Security Issue</th>
<th>Impact on Cloud System</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security</td>
<td>Information misfortune, phishing, botnet (running remotely on a gathering of machines) posture genuine dangers</td>
<td>Vulnerable security threats</td>
<td>Strong encryption technique should be used and use fine grained access</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cost</th>
<th>Impact on Cloud System</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td>This issue is especially noticeable if the buyer utilizes the hybrid cloud sending model where the association's information is conveyed among various open/private (in-house IT foundation)/group clouds</td>
<td>Limited use of Cloud</td>
<td>Depends upon the usage of cloud and its resources.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Charging</th>
<th>Impact on Cloud System</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td>More Availability but less users due to higher cost charges</td>
<td>Limited use of cloud services (SaaS)</td>
<td>Depends upon the requirement of user.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service level agreement</th>
<th>Impact on Cloud System</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td>issue is the meaning of SLA determinations in a manner that has a suitable level of granularity, to be specific the tradeoffs amongst expressiveness and complicatedness, with the goal that they can cover a large portion of the customer desires.</td>
<td>Trust issues</td>
<td>Only trusted employees should given the rights to use SLA</td>
</tr>
</tbody>
</table>
Cloud interoperability issue

Driving merchant locking, which precludes the capacity of clients to look over option sellers/offering at the same time so as to streamline assets at various levels inside an association.

More vitally, restrictive cloud APIs make it extremely hard to coordinate cloud administrations with an association's own current legacy frameworks.

End goal of enhancement, an association may need to outsource various negligible capacities to cloud administrations advertised by various sellers.

CONCLUSION

As described in the paper, though there are extreme advantages in using a cloud-based system, there are yet many practical problems which have to be solved. Cloud computing is a disruptive technology with profound implications not only for Internet services but also for the IT sector as a whole. Still, several outstanding issues exist, particularly related security and privacy. As described in the paper, currently security has lot of loose ends which scares away a lot of potential users. Until a proper security module is not in place, potential users will not be able to leverage the advantages of this technology. In this paper, we presented a selection of issues of Cloud Computing security. We investigated ongoing issues with application of XML Signature and the Web Services security frameworks, discussed the importance and capabilities of browser security in the Cloud Computing context (SaaS), data security issues in SaaS, security issues in PaaS and we suggested some countermeasures to avoid the data loss and for making the cloud computing more secure.

References


8) Hassan Rasheed in “Data and infrastructure security auditing in cloud computing environments.” Taif University Deanship of Information Technology, Saudi Arabia.

12) S. Subashini V. Kavitha in “A survey on security issues in service delivery models of cloud computing” Anna University Tirunelveli, Tirunelveli, TN 627007, India.