© 2018 IJSRST | Volume 4 | Issue 7 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Security issues in Networks Using SSL Algorithm in Cloud Computing

P. Mani[1], A. J. Rajasekhar[2]
[1]Student, Department of MCA, SVIM, Tirupati, Andhra Pradesh, India
[2]Assistant Professor, Department of MCA, SVIM, Tirupati, India

ABSTRACT

Cloud computing is a style of processing in which business gives application information and any sort of IT resource as a service to customer. To access services of cloud computing you just need Internet get to? Cloud computing is obviously one of the present most luring innovation territories because of its cost-efficiency and adaptability. Be that as it may, with this offices it isn't picking up as much prevalence as it must be, a large portion of the association are not have any desire to send cloud condition. Security is one of the real issues which lessens the development of cloud computing. In this paper we portray how the association can convey this processing condition without being stressed over security issues.

Keywords : SaaS, IaaS, PaaS, Multi-tenant, Security, SSL.

I. INTRODUCTION

Cloud computing is a style of registering in which business forms, application, information and any kind of IT resource can be given as a support of the client. It is a build that enables you to get to applications that really dwells at an area other than your PC or other web associated gadget. Cloud computing get its name as an allegory for the web. Commonly, the web is spoken to in organize chart as a cloud. (A similitude is an innovative method for depicting something by alluding to something unique which is the same especially. Cloud computing has turned into a noteworthy innovation drift, and numerous specialists expect that cloud computing will reshape IT forms and the IT commercial center. Cloud computing enables buyers and organizations to utilize applications without establishment and access their own records at any PC with web get to. This innovation takes into account considerably more effective computing by unifying stockpiling, memory, handling and data transmission.

Services: Services in cloud computing is the idea of having the capacity to utilize reusable and fine grained segment over a seller's system. This is broadly referred to "as a service". Offering with as services as an addition incorporate qualities like after:

1. Low hindrances to section, making them accessible to independent companies.
2. Substantial versatility.
3. Multi-tenure, which enable resources to be shared by numerous clients.
4. Device independence, which enables client to get to the frameworks on various equipment.

Services of cloud computing is partitioned in following three classifications:

1. Software as a Service. (SaaS)
2. Platform as a Service. (PaaS)
3. Infrastructure as a Service. (IaaS)

Software as a Service Software as a Service (SaaS) is a model in which an application is facilitated as

a support of clients who get to it by means of Internet. At the point when the product is facilitated off-site, the client doesn't need to look after it. Then again, it is out of client's hands when the facilitating service chooses to transform it. The thought is to utilize the product out of the case as is and don't have to roll out a great deal of improvements or expect incorporation to other framework. Cost can be an essential factor in this computing condition for getting to any product, as opposed to pay for it once and be finished with it , the more you utilize it ,the more you should ("pay-for-utilize"). SaaS gives organize based access to financially accessible software. Since the product is overseen at a focal area, clients can get to their application wherever they have web get to.

Platform as a Service Platform as a Service (PaaS) is another application conveyance display that gives every one of the resources required to manufacture application and services totally from the Internet, without downloading or introduce software. PaaS services incorporate application outline, advancement, testing, arrangement and facilitating. Different services incorporate group joint effort, web benefit mix, security, adaptability, stockpiling, state service and forming. PaaS by and large offered some help to help.

Infrastructure as a Service: Infrastructure as a service is the following type of services accessible in cloud computing. Where SaaS, PaaS are giving applications to clients, IaaS doesn't. It basically offers the equipment so your association can put whatever they need onto it. As opposed to buy server s, software racks, and paying for the datacenter space for them, the specialist co-op rents those resources.

II. Characteristics of Cloud Computing

Following are the five fundamental qualities of cloud computing:

On request self services: Computer services, for example, email, applications, system or server service can be furnished without requiring human cooperation with each specialist co-op. Cloud specialist organizations giving on request self services incorporate Amazon Web Services (AWS), Microsoft, Google, IBM and Salesforce.com.

Broad network access: Cloud Capabilities are accessible over the system and got to through standard components that advance use by heterogeneous thin or thick customer stages, for example, cell phones, PCs and PDAs.

Resource pooling: The supplier's processing resources are pooled together to serve various customers utilizing numerous occupants demonstrate, with various physical and virtual resources powerfully allotted and reassigned by purchaser request. The resources incorporate among others stockpiling, handling, memory, arrange data transfer capacity, virtual machines and email services.

Rapid elasticity: Cloud services can be quickly and flexibly provisioned, now and again consequently, to rapidly scale out and quickly discharged to rapidly scale in. To the shopper, the abilities accessible for provisioning frequently give off an impression of being boundless and can be bought in any amount whenever. Estimated benefit: Cloud registering resource use can be estimated, controlled, and detailed giving straightforwardness to both the supplier and buyer of the used service.

Deployment Model: Deployment of cloud computing can rely upon the prerequisite and

distinguishes as following four writes which is likewise appeared in figure. Public cloud: Public cloud depicts cloud computing in the customary standard sense, whereby resources are powerfully provisioned to the overall population on a fine-grained, self service premise over the Internet, by means of web applications/web services, from an off-website outsider supplier who charges on a fine-grained utility registering premise.

Private cloud: Private cloud is framework worked exclusively for a solitary association, regardless of whether oversaw inside or by a third party and facilitated inside or remotely. They have pulled in feedback since clients "still need to purchase, assemble, and oversee them" and in this way don't profit by bring down forthright capital expenses and less involved service, basically "[lacking] the monetary model that makes cloud computing such a captivating idea". Group cloud: Community cloud shares foundation between a few associations from a particular group with basic concerns (security, consistence, locale, and so on.), regardless of whether oversaw inside or by an outsider and facilitated inside or remotely. The expenses are spread over less clients than a public cloud (however in excess of a private cloud), so just a portion of the advantages of cloud computing are figured it out.

Hybrid cloud: Hybrid cloud is a structure of at least two clouds (private, group, or public) that stay one of a kind elements however are bound together, offering the advantages of various arrangement models. It can likewise be characterized as a numerous cloud frameworks that are associated in a way that enables projects and information to be moved effectively starting with one arrangement framework then onto the next.

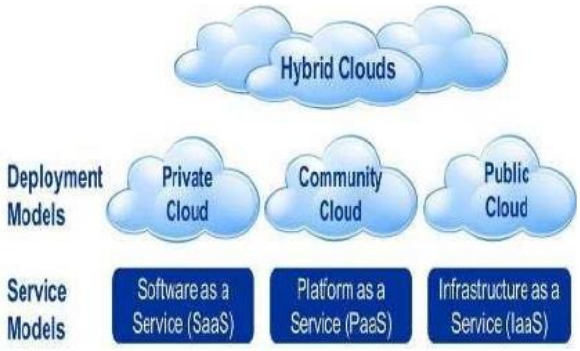

Figure 1. Service and Deployment Models of Cloud

III. Cloud Security Issues

In the cloud computing the customer stores its information to the area about which he doesn't know anything and subsequently some kind of security instrument is expected to guarantee the customer for not being stressed over its information. A current study by Cloud Security Alliance (CSA) and IEEE shows that numerous association is wont to execute cloud computing yet they require the security arrangement. Security in the cloud computing condition can be distinguishes as following:

1. Security in SaaS.
2. Security in PaaS.
3. Security in HaaS.

In this paper we are speaking to arrange security; along these lines we will have brief look on security in SaaS. Despite the fact that SaaS offer incredible focal points to the customers yet there are some security issues are identified with it. In SaaS, the customer needs to rely upon the supplier for appropriate safety efforts. The Cloud Service Provider (CSP) needs to guarantee the customer about security. The accompanying key security issues ought to be considered as indispensable piece of SaaS execution.

1. Data Security.

2. Network Security.
3. Data locality.
4. Authentication and Authorization.

Data Security: Data security is the methods for guaranteeing that information is remained careful from debasement and that entrance to it is appropriately controlled. Along these lines information security guarantees protection. It additionally helps in ensuring individual information. In a conventional application arrangement show, the imperative information of every association keeps on dwelling inside the association limit and is liable to its physical, coherent and faculty security and access control strategies. In any case, in the SaaS show, the association information is put away outside the association limit, at the SaaS specialist co-op end. In this way the specialist organization needs to utilize methods, for example, encryption, solid client verification and go down for giving information security.

Network Security: In the cloud computing condition every one of the information moves through the web that is subjected to impact by different sort of assaults. In this manner the specialist co-op needs to utilize some system security component. In the following area of the paper we will have detail look on organize security.

Data locality: In a cloud domain, the buyers utilize the applications gave by the SaaS and process their business information. In any case, the client does not know where the information is getting put away. In numerous a cases, this can be an issue. Because of consistence and information protection laws in different nations, region of information is of significance in numerous associations design. For instance, in numerous EU and South America nations, certain sorts of information can't leave the nation due to possibly touchy data. Notwithstanding the issue of neighborhood laws, there's additionally the subject of whose locale the information falls under, when an examination happens. A protected SaaS show must be equipped for giving dependability to the client on the area of the information of the purchaser.

Authentication and Authorization: Because in the application and information is facilitated outside of the association in the cloud computing condition, the cloud specialist organization needs to utilize Authentication and Authorization system.

IV. Network Security

In cloud information stockpiling framework, clients store their information in the cloud and never again have the information locally. In this way, the accuracy and accessibility of the information documents being put away on the dispersed cloud servers must be ensured. In cloud computing all information streams over the web should be secure with a specific end goal to avoid so as anticipating spillage of delicate information. This includes the utilization of solid system activity encryption strategies, for example, Secure Socket Layer (SSL) and the Transport Layer Security (TLS) for security. SSL (Secure Socket Layer) is a convention created by Netscape that empowers a web program and a web server to convey safely; it enables the web program to confirm the web server. SSL remains for Secure Sockets Layer convention created by Netscape and is the standard Internet convention for secure correspondences. The safe hypertext transfer protocol (HTTPS) is a correspondences convention intended to exchange scrambled data

between PCs over the World Wide Web. HTTPS is http using a Secure Socket Layer (SSL). A protected attachment layer is an encryption convention conjured on a Web server that utilizations HTTPS. SSL is a sort of attachments correspondence and dwells between TCP/IP and upper layer applications, requiring no progressions to the application layer.

The SSL convention incorporates two sub-conventions: the SSL record convention and the SSL handshake convention. The SSL record convention characterizes the configuration used to transmit data.

The situation of SSL convention is appeared in figure:-

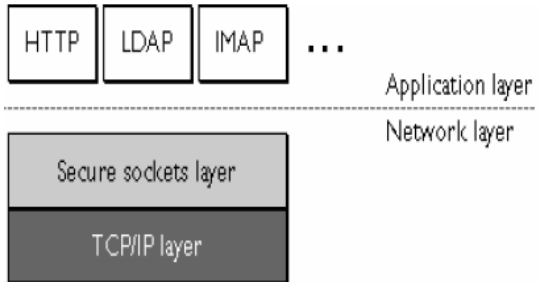

Figure2. System Security of Cloud

SSL handshake convention includes utilizing the SSL record convention to trade a progression of messages between a SSL-empowered server and a SSL-empowered customer when they initially build up a SSL association. This trade of messages is intended to encourage the accompanying activities:

- ✓ Authenticate the server to the customer.
- ✓ Allow the customer and server to choose the cryptographic algorithms, or figures, that they both help.
- ✓ Optionally validate the customer to the server.
- ✓ Use public key encryption procedures to produce shared secretly
- ✓ Establish an encoded SSL association.

SSL innovation is utilized to set up a safe and encoded correspondence channel between two Internets associated gadgets. The SSL convention utilizes RSA algorithm which is a public key algorithm for encryption and decoding created by Rivest, Shamir, and Adleman. SSL convention likewise utilizes idea of Certificates. Authentications are computerized archives bearing witness to the official of a public key to an individual or other element. A SSL authentication contains the accompanying data:

1. The space for which the testament was issued.
2. The proprietor of the testament (who is the additionally the individual/element who has the privilege to utilize the area).
3. The physical area of the proprietor.
4. The legitimacy dates of the endorsement. SSL gives trust in the uprightness and security in arrange framework. Customers are winding up progressively mindful of the benefits of SSL security.

V. Conclusion

In this paper we depicts the security issues identified with the cloud computing. We indicate how the association can guarantee information insurance and send this condition. We likewise demonstrate the significance of encryption. For giving answer for this security issues we depend on Secure Socket Layer Protocol which depends on RSA algorithm for encryption and unscrambling of information which course through web.

VI. REFERENCES

[1]. Deep Vardhan Bhatt, Stefan Schulze, Gerhard P. Hancke(2006) "Secure Internet Access to Gateway Using Secure Socket Layer" ieee transactions on instrumentation and measurement, vol. 55, no. 3.

[2]. Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacono (2009) "On Technical Security Issues in Cloud Computing" IEEE International Conference on Cloud Computing.

[3]. Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou (2009) "Ensuring Data Storage Security in Cloud Computing".

[4]. C. Coarfa, P. Druschel, and D. S. Wallach. Performance Analysis of TLS Web Servers. ACM Trans. Comput. Syst., 24(1):39–69, Feb. 2006.

[5]. Common Vulnerabilities and Exposures. CVE-2014-0160. Available at: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160.

[6]. Comodo. Report of incident on 15-mar-2011. Technical report, March 2011. Available at: https://www.comodo.com/ Comodo-Fraud-Incident-2011-03-23.html.

[7]. Crossbear Project. SSL Landscape - X.509 data sets. Available at: https://pki.net.in.tum.de/node/8.

[8]. Subedari Mithila, P. Pradeep Kumar (2011) "Data Security through Confidentiality in Cloud Computing Environment" International Journal of Computer Science and Information Technologies, Vol. 2 (5), 1836-1840.

[9]. M S.Bhiogade (2002) "Secure Socket Layer" Informing Science InSITE - "Where Parallels Intersect".

[10]. Amit Batra, Rajender Kumar, Arvind Kumar (2011) "A Review of Storage and Fault ToleranceApproaches Used in Cloud Computing" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (5), 2011, 1971-1978.

[11]. J. Leyden. Step into the BREACH: HTTPS encrypted web cracked in 30 seconds. The Register, August 2013. Available at: www.theregister.co.uk/2013/08/02/breach crypto attack.

[12]. E. Mills. Go Daddy-serviced Web sites go down; hacker takes credit. CNET, September 2012. Available at: http://www.cnet.com/news/godaddy-serviced-web-sites-go-down-hacker-takes-credit.

[13]. Netcraft. Phishing Alerts for SSL Certificate Authorities. Available at: http://news.netcraft.com/archives/2012/08/22/phishing-on-sitesusing-ssl-certificates.html.

[14]. Public Web Application Security Project. Testing for SSL-TLS (OWASP-CM-001). Available at: https://www.owasp.org/index.php/Testing for SSL-TLS (OWASPCM-001).

[15]. P. Eckersley and J. Burns. An observatory for the SSLiverse, July 2010. Talk at DEFCON '18. Available at: https://www.eff.org/files/DefconSSLiverse.pdf.

[16]. P. Eckersley and J. Burns. Is the SSLiverse a safe place, 2010. Talk at 27C3.

About Authors:

Mr.P.Mani is currently pursuing his Master of computer Applications, SVIM, Tirupati, AP.

Mr.A.J.Rajasekhar is currently working as an Assistant Professor in MCA Department, SVIM, Tirupati, AP.