International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 6, September-October 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Security Issues on SAAS Model of Cloud Computing

Vikas Kumar[1], Ms. Deepali Shahane[2]

[1]Student, [2]Assistant Professor,

[1,2]Bharati Vidyapeeth Institute of Management and Information Technology, Navi Mumbai, Maharashtra, India

ABSTRACT

Cloud computing nowadays, In IT trade has become unsecure. Its impact on various business application is threat for our organization. Multiple options that create cloud computing enticing have simply defiance the prevailing security system; however, they uncover new security problems. This paper provides an information about challenges and issues that we face while using cloud software's or applications.

KEYWORDS: *Cloud Computing, Insecurity in SAAS, ancient Security Issues*

How to cite this paper: Vikas Kumar | Ms. Deepali Shahane "Security Issues on SAAS Model of Cloud Computing" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-6, October 2020, pp.423-425, URL: www.ijtsrd.com/papers/ijtsrd33379.pdf

IJTSRD33379

1. INTRODUCTION

Many experts and researcher written about cloud computing and they believe that it's a revolutionary change in the history of internet. Consistent with Gartner [1], cloud computing can be describe as - a form of computing in which different web based application are used by the client who make use of web technologies. consistent with the Sercombe [2] and National Institute of Standards & Technology [3], Cloud computing include SAAS (software as a service) and more three cloud delivery model. Software as a service in which service provider host the application within its datacenter and provide license to users for using this application over internet. The main aim of this paper is to focus on the security issues of cloud delivery model.

2. MISTAKES AND REALITY

Now cloud computing proved that cloud based application are most advance and revolutionary initiative in information technology. cloud based application are available at very low cost and easy to use, but on the other hand we think that it breach our personal data. Many businesses depend on their service provider who host web application and provide their confidential data to service provider which encourage the data breaching.

3. SECURITY ISSUES IN SAAS

In SAAS concept, business completely depend on service provider and think that service provider takes all precautions to protect their data, but instead businesses must ensure the right security measures [4]. According to the definition of SAAS, when client move from old application to new application. Then, he need to ensure about new application safety measures and condition instead of focusing on application replacement [2]. Client Data is available on database which is host by the application vendor. Service provider can use private server or can use public server for to deploy their application (e.g Google or Amazon etc.) Sometimes service provider store data on different server to maintain availability of data which challenge the security of data.

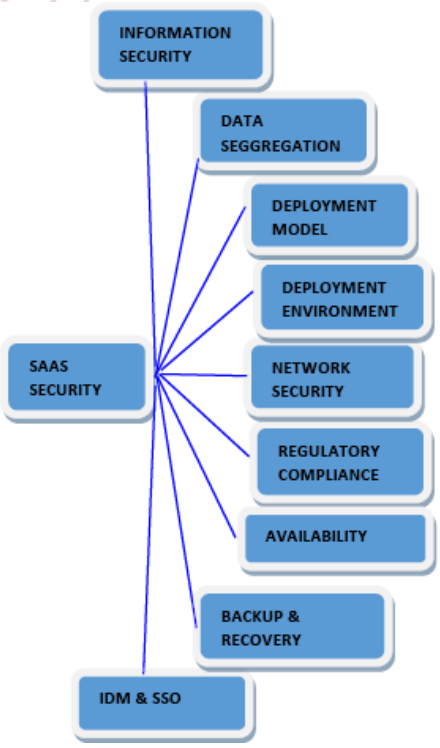

Figure 1: Security problems in field of SaaS by Kannan Subbiah [22]

3.1. Former Security Challenges

Some Old communication security challenges also applied to cloud computing. Cloud computing generate some new security threat, but some old security problems also affect cloud computing.

3.1.1. Validation

Validating credential system for corporate use is very essential and need some update to meet security requirements. Some task are become very hard to perform because system is present on cloud.

3.1.2. Availableness

The availability of data at the time of need played very crucial role in cloud computing. Service provider mainly focus on availability of data. To ensure Fetching and delivery of data should be faster, service provider store data on different server and also maintain speed of internet.

3.1.3. Information privacy

Information privacy can be define as the precaution of unapproved leak of information. Privacy in terms of cloud computing refer to copy rights of essential information or any pictures etc. [10]. SAAS include fetching and delivery of data from cloud server through internet which is host by the service provider. Fetching and deliver of data may include text, videos, pictures etc.

3.1.4. Virtual Machine Concern

Virtualization is temporary revolutionary change in information technology. As virtualization increasing day by day generating more threat to data privacy [6]. Different machines used for virtualization may have vulnerable, as exemplified by [7] Such unsecure machine can affect the all users in terms of data privacy. One of the most usable elements of a cloud is virtualization. However, this generates major security risks & problems. At same time different applications running on same machine which is the example of virtualization.

3.2. CHALLENGES IN CLOUD COMPUTING

3.2.1. Network Privacy

When fetching and delivery of data takes place takes place between user and vendor through internet network that network must be secured as per latest terms and condition. This network must include encryption techniques. This kind of techniques include security protocol which encrypt data between browser and server like SSL (Secure Socket Layer Security) and TSL (Transport Socket Layer Security) [8]. However, many unauthorized user can steal data if network is weak or unsecure.

3.2.2. Resource spot

When users registered with provider for particular web application without even knowing where the machines are located for that particular services. As we already know about that different countries have different laws for cyber-crime. [9]. Many standards or policies are published by European union in the interest of customers to protect customer privacy in information technology under 95/46/EC [10]. Different countries have different rules which is not applied on other country and does not guarantee the security of data for that particular country.

3.2.3. SAAS model standards

To make stability between users and provider there are some standards in cloud computing. Standards that created for the welfare of both customer and provider, Following standards are listed in the field of cloud computing list as follows IEEE Cloud Model Usual Study cluster [11], ITU Cloud Computing Focus cluster [12], Cloud Safety Alliance (CSA), Distributed Management Task Force [13], and Storage Networking trade Association [14].

3.2.4. Fetching of Data

Fetching of data from cloud server in different organization has different security standards. In particular organization different data restrictions are applied to different level of employee. [15]. These standards are made to protect any unsecure access of data [16]. The Cloud model policies must be mature to accept the policies of particular organization as per security concern.

3.2.5. Internet application privacy

SAAS is a encrypted format that place on network. When users request data from cloud the request is encrypted and travel through secure network to destination. Server send encrypted reply to users. Any malicious user can steal data if data is travel through unsecure network. Most important requirement of saas is internet [17]. The encrypted data as a service resides within the cloud while not moorage with the particular users. When data is requested by particular user then available data within the cloud modified and sent to user [18]. All this process of data encryption and decryption challenge data privacy.

3.2.6. Information Security Concern

Multiple organizations and businesses data are available on cloud at same time if any attack to cloud environment then it put all the organizations data at risk [20].

3.2.7. Cloud Security Agreement (CSA)

CSA contract contain multiple standards for the welfare of both client and provider which include quality of service, On time delivery, Security of Data etc. When Company or Organization sign cloud security agreement they need to go through entire agreement for security reasons. Otherwise incomplete knowledge about agreement can lead to security threat.

4. CURRENT SECURITY SOLUTIONS

There are many researcher doing research for the security of cloud computing. Multiple organizations or business want to invent new security policies and standards in the area of cloud computing. There are multiple organization that allow the individual to take part in the discussion of cloud security on existing and future solution. [5].

Sr. No.	Security Fields	Existing/Future Solutions
1	Validations	➢ Two Methods Validations.
2	Accessibility	➢ Data Distribution.
3	Information privacy	➢ Attribute primarily based Proxy Re-encryption.
4	Virtual Machine Safety	➢ Keep updating your physical machine ➢ Analysis on Virtual Machine Safety.
5	Data Privacy	➢ Data Privacy Threat managing Structure.
6	Internet Safety	➢ Encrypted Web Safety for between user and provider.
7	Web Application policies	➢ Adoption of some old communication policies. ➢ Enhancement from data security point of view.
8	Requesting or exchanging information on cloud	➢ Multiple request handling. ➢ Managing information request structure.
9	Protection of saas services	➢ Antivirus for online services.

Table 1: Current solutions accessible in the area of cloud computing

5. CONCLUSION

Undoubtedly, cloud computing prove that it has numerous advantage, but on other side some problems need solution. At current stage IT sector more dependent on cloud based application, then also many issues remain untouched on which need to be sorted. Many changes require in Cloud security agreement for the welfare of users and provider. As well as there is need of some cloud security global policies which will applied to all over the world.

REFERENCES

[1] Heiser J. (2009) what you want to grasp concerning cloud computing security and compliance, Gartner, Research, ID Number: G00168345.

[2] Seccombe A.., Hutton A, Meisel A, Windel A, Mohammed A, Licciardi A, (2009). Security steering for crucial areas of focus in cloud computing, v2.1 Cloud Security Alliance, 25 p

[3] Mell P, Grance T (2011) The National Institute of Standards and Technology definition of Cloud Computing. NIST, Special Publication 800–

[4] Choudhary V. (2007). A coding system as a service: implications for investment in coding system development. In: International conference on system sciences, 2007, p. 209.

[5] Cloud Security Alliance. Security steering for crucial areas of focus in cloud computing Version2.1.(2009), http://www.cloudsecurityalliace.org/guidance/csaguide.pdf

[6] Amazon. Amazon Elastic reason Cloud (EC2).

[7] Secunia. Xen multiple vulnerabilities; 2011

[8] Amazon. Amazon Elastic reason Cloud (EC2), 2010 /http://www.amazon.com/ ec2/S

[9] Soft layer. Service Level Agreement and Master Service Agreement, 2009 http://www.softlayer.com/sla.html

[10] World organization. Directive 95/46/EC of the European Parliament and of the council of twenty-four Gregorian calendar month 1995 on the protection of individuals with connectedness the method of personal data and on the free movement of such data; 1995.

[11] IEEE CCSSG. IEEE Cloud Computing traditional Study cluster

[12] ITU, 2013. Cloud Computing Focus cluster.

[13] DTMF, 2013.Distributed Management Task Force. .[Accessed: Jan 2013]

[14] SNIA. (2013).Storage networking business Association.

[15] Kormann D, Rubin A. (2000) Risks of the passport single sign-on protocol. Computer Networks 2000; thirty 3 (16) : 51–8.

[16] Blaze M, FeFeigenbaum J, Ioannidis J, Keromytis AD. The role of trust management in distributed systems security, secure net programming, problems for mobile and distributed objects. Berlin: Springer-Verlag; 1999.p.185–210

[17] Zalewski M. Browsers security handbook, 2009 /http://code.google.com/p/browsersec/S.

[18] Subashini S, Kavitha V. A survey on security problems in commission delivery models of cloud computing. J Network Comput Appl (2010), DOI:10.1016/j.jnca.2010.07.006

[19] OWASP. (2010) The 10 most crucial internet application Security risks https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[20] Claude Bernard Golden. Shaping non-public clouds, 2009/http://www.cio.com/article/492695/Defining_Private_Clouds_Part_One

[21] Raj H, Nathuji R, Singh A, England P. Resource management for isolation increased cloud services. In: Proceedings of the 2009 ACM workshop on cloud computing security, Chicago, Illinois, USA, 2009P.

[22] SecurityIssues.https://pt.slideshare.net/goldsun/saas-challenges-security-concerns-11054493/18