A Review on Cloud Computing Security and Privacy in Service Oriented Architecture (SOA)

Surbhi Sharma[1] Ashish Guwalani[2], Akansha Jain[3]
[1,2] Asst. Professor, Department of Computer Science and Engg, ACERC, Ajmer,Rajasthan
surbhi2690@gmail.com,ashuashu2322@gmail.com
[3]M.Tech Scholar, Department of Computer Science, MDSU, Ajmer, Rajasthan
jain1994aakanksha@gmail.com

ABSTRACT

Cloud computing is powerful computing which is transformed the traditional computing and industries. Cloud is not a new concept. Many organizations like Google, Microsoft, and Amazon accelerate in developing this computing and provide the services for lots of users and storing the data through cloud now become a norm. But there are many issues that arrive to store the data in cloud. In this paper we review some securities issues and give a survey solution that have been done to minimize the security risk and describe future research work about all these risk that occur when data is stored in cloud computing.

DOI : https://doi.org/10.30991/IJMLNCE.2017v01i02.004

KEYWORDS

Cloud Security, Threats, Data Security Availability, Privacy , SOA

1. Introduction

Cloud in its evolution form has been changed era wise as we see in the past era. From the begging when mainframe were predicting to be the future of computing. Cloud computing turned from higher and expensive to smaller personnel computer and Server are used to construct cloud computing and it is also called cloud. cloud computing is an advanced and latest terminology in which availed resources are used for data stored over cloud computing purpose and these sharable resources are not externally located at the user location like Amazon Web services which is extremely secure web service as well as user or enterprises store their personal data via its simple storage service (S3)[1]but their logical significance meant it for particular cloud.

In display time little and expansive association are utilizing distributed computing and in the wake of utilizing cloud they can increase quick access to all applications and lift their framework assets at extremely least cost (Gartner, Jay heiser 2009) The cloud benefit gives directly heaps of chance in the market the administration gives must protect that they get the security viewpoint. Distributed computing is centred on conveying administrations and significance of distributed computing is expanding in colossal market. Distributed computing

was characterize by NIST "distributed computing is show for empowering, helpful on request arrange access to shared pool of registering asset (eg systems, server stockpiling, application benefit)" that can be vastly provisioned and admitted with insignificant administration exertion.

Figure 1.1 Model Architecture of Cloud Computing

Fundamental qualities of distributed computing :[2][22]

On Demand Self Service: A user can significantly require resources on the demand by secured oriented architecture, for example, server time usability and network storage space as required by the cloud without requiring individual user collaboration with each specialist co-op's.

Resource pooling: The cloud supplier to serve multiple copies of flexible and sharable resources for requested users, with different physical and virtual resources. These sharable resources are repeatedly assigned and reassigned by the cloud supplier to the cloud users. There is wide availability of area for the requisites and these requisites has no control or information over the correct area of the cloud but multiple resources ensure that they might have the capacity to indicate area at a larger amount of reflection over wide geographical region over cities and country range. Available resources had their own huge capacity, flexibility, preemptiveness, internal memory, arrange transmission capacity, and virtual machines.

Broad Network Access: Distributed Computing, Grid Computing and cloud computing all concepts are available over the wide range of network using many kind of standard mechanism for their heterogeneous thick and thin clients platforms (like smart phone, Tablet, Palmtop, Personal Digital Assistant)

Rapid Elasticity: Cloud Computing platform has capabilities that can be fastest flexibility, somehow its manually upgradable towards for scale out and vice versa. To the user, the capabilities available for providing often resembled to be limitless and can be brought in wanted quantity at any time.Measured Service: Cloud Infrastructure design in such way that they manage advanced and widely available sharable resource uses by utilizing a measuring capability at some level of threshold suitable to the sort of service (e.g., stockpiling, preparing, transfer speed, and dynamic client accounts).Resource used by user can be managed, controlled, and announced giving straightforwardness to both the supplier and buyer of the used administration.

Distributed computing has three administration show (SaaS, IaaS, PaaS) and for sending model (Public private group and cross breed).

Figure 1.2 Cloud Computing Characteristics

Cloud service running somewhere in the cloud computing infrastructure through internet, cloud computing allow provide to develop, deploy and run the application that can easily grow in capacity, performance and never fall reliability. The penalty of obtaining these properties of cloud computing are to store the private data on the other site of internet and get services from other parties [15].

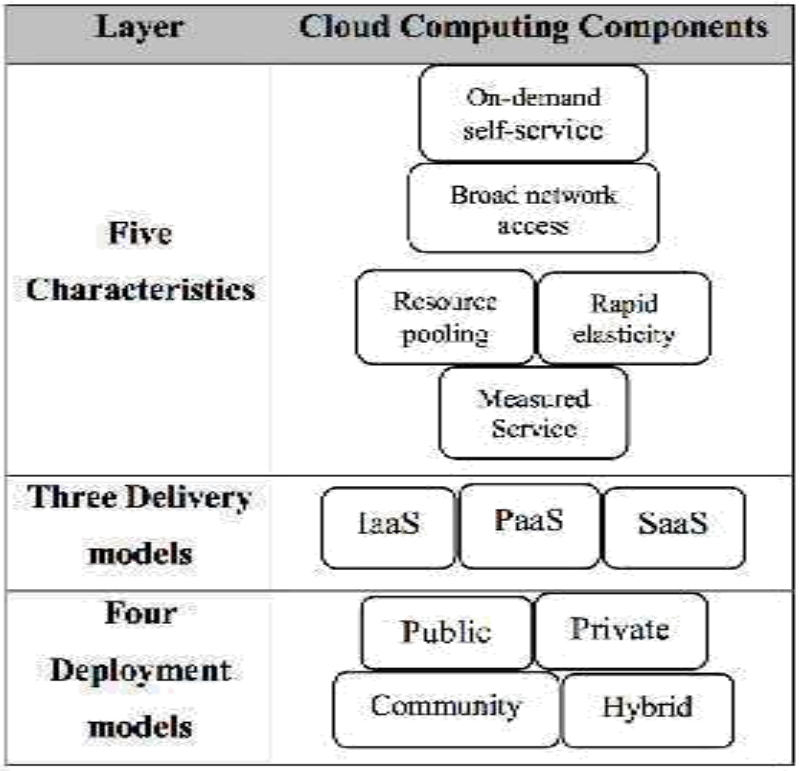

Figure 1.3 : Cloud Computing Layered Architecture

2. Cloud Security Issues

Indeed, even with their many advantages of distributed computing, already keep up clients are hesitant to receive this innovation and move from customary processing to distributed computing. [3] In distributed computing, security is an expansive theme. It is a blend of advances, controls to shield the information, and arrangements to ensure the information, administrations, and framework. This blend is an objective of conceivable assaults. In this manner, there are updated and vast security necessities in the cloud infrastructure conflicted with old and traditional security design is divided on the basis that the client mandatory conditions. It doesn't ensure that the basis many more. Similarly, the common security and privacy of cloud-based framework is similar to the security of the least substance [4]. By

outsourcing, users leave their physical control over the data when it is put away in a remote server and they allotted their control to an untrusted cloud supplier or groups [5], [6]. In the range of capable and dependable server contrasted with user applied force and unexpected quality, there are a wide range of dangers confronting the cloud from vulnerabilities as well as from an in depth which can use cloud vulnerabilities to do harm [7]. These dangers may risk information classification, information respectability, and information accessibility. Some untrusted suppliers could conceal information ruptures to spend their notations or released some storage space that the minimum utilized or got to information.

2.1 Security in Service Models of the cloud

Cloud computing has three service model as given by NIST [2] by which different type of services are available for the user/client. The three services model SaaS, PaaS, IaaS. Which provide software as a service, platform as a service and infrastructure as a service to the client.

A recent study by CSA [20] represent that the different industries and organizations across sector are interested to adopt cloud computing.

i. SaaS is a software deployment model for cloud service infrastructure where application is remotely hosted by service provider. SaaS is rapidly evolved as the delivery model for meeting the need of technology related Services. Some enterprises are not sounded with the SaaS model due to minimization of visibly about the method their data is stored and secured.

ii. IaaS is providing the infrastructure for enterprises and it totally changed the way developer deploy the application, instead of spending big investment with their own data centre or manage hosting companies .

iii. PaaS is the platform as a service and it is the layer which reside above on the stack of IaaS. PaaS generates the set of developing environment that a developer can build their application without having any idea about what is going in the services. PaaS offers developers are service that provides a software development life cycle from planning to deployment and testing to maintenance.

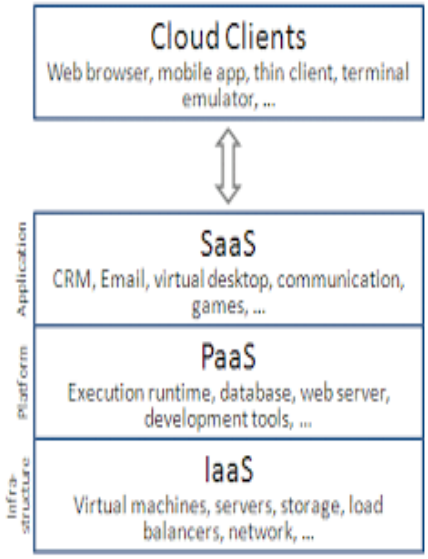

Figure 2.1 : Cloud Service Models

Figure 2.2: Components of Cloud

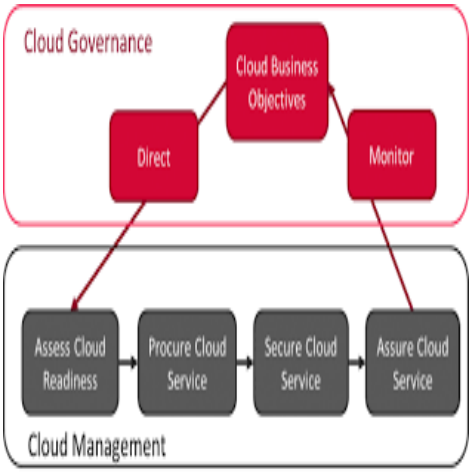

Figure 2.3 : Cloud Security Model

Numerous security and protection episode are see in distributed computing framework, we have recorded some of them A sales force utilize succumbed to a phishing assault and released a client's rundown, which produced facilitate phishing assault on October 2007.Google docs found a stream that in antagonistically share client dock in walk 2009. There are a few securities components are considered as a major aspect of the SaaS application.

i. Data security
ii. Data Classification
iii. Data area
iv. Data trustworthiness
v. Availability Authorization
vi. Authentication Data Repudiation
vii. Back-up

Figure 2.4 : Key Security Elements

3. Secutity Threats In Cloud Computing

Cloud Computing architecture is comprised a servers with huge amount of data over server either in the form of structured or unstructured way. Presently there are many threats related to the security of cloud, these are:

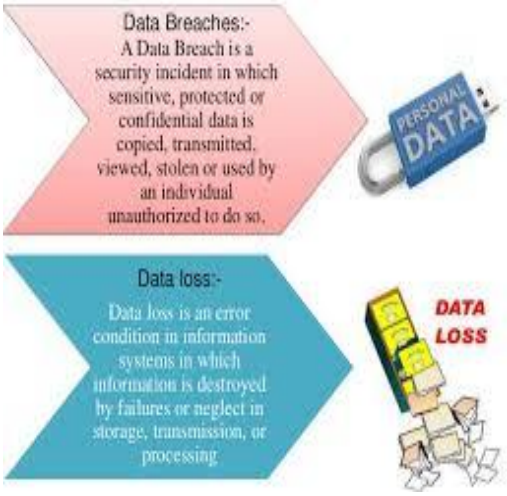

Fig.3.1 Security Threats in Cloud Computing

Data Loss :- Industries and enterprises are outsourcing their data to cloud service provider because of minimum range of cost rate that the cloud offers the users should advertised their cloud data on their behalf with some issues related to the security and there are some risk includes like lack of integrity, lack of accessibility and lack of potentiates. There are various types of attacks over the server like nonrepudiation, denial of service etc. are directly related to the data loss. These losses could generate a risk of server crash which may not be easily recovered by the providers.

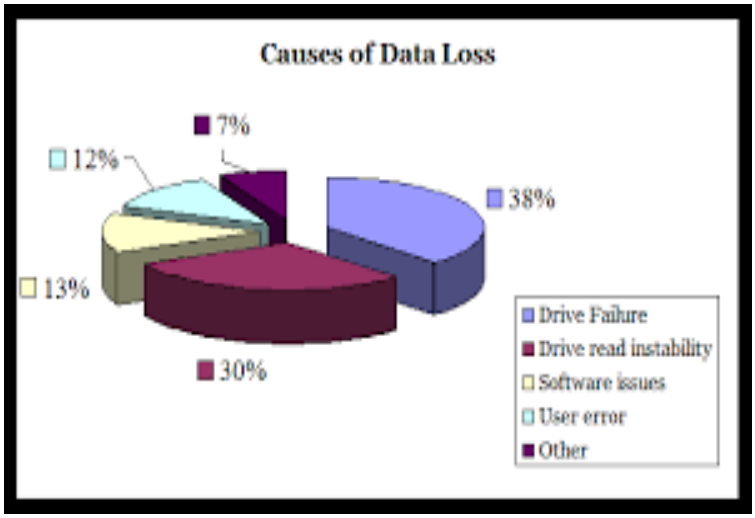

Figure 3.2 : Causes of Data Loss

Data Breaches:- In the distributed computing, the administration has different clients whose information are put away in some put. Any rupture to the cloud condition would uncovered all the client information unclosed [9] on account of a multi-occupancy, client utilizing diverse application on virtual machine and could share some database and every one of the information break was accounted for in information rupture examination report (DBIR)2013,2014 that hacking a malware regular reason for information rupture [12].

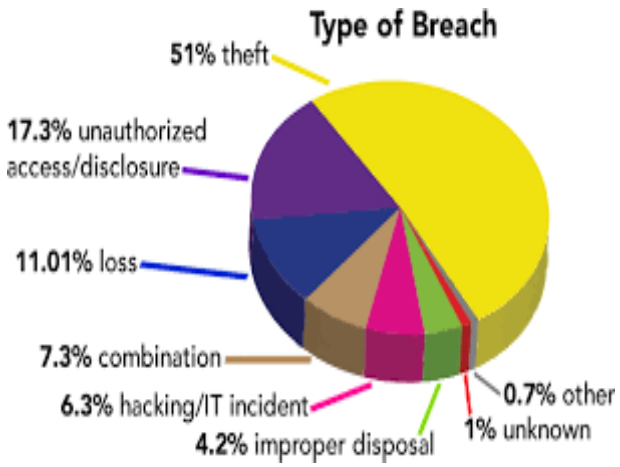

Figure 3.3 Data Breaches types

Availability:- The motivation behind accessibility for distributed computing is to guarantee that its client/customer can utilize them at a whenever and at wherever. Cloud framework empower its client to get to the framework from anyplace. Multitier design should be embraced, bolstered by stack adjusted, running on a variable quantities of servers. Many distributed

computing framework give cloud foundation in light of virtual machine. Eg Amazon/web Service give EC2.Amazon keep up basic data transfer capacity this surpasses it gives supply web transmission capacity. These whole evaluation tests approve the accessibility like verification shortcoming, session administration [9] [10].

Integrity:- Data uprightness is effectively kept up in independent framework with single database. Information uprightness in such a framework is kept up by means of database imperatives an exchanges. Exchange ought to take after ACID (atomicity, consistency, confinement, Durability) properties to guaranteed uprightness. The absence of trustworthiness controlled at the information level could bring about significant issues. To keep up the respectability Zetta was presented by which primarily center in information honesty which has comparative plan to RAID framework [13] [14].

i. Audit:- Review intends to watch what occurred in the cloud framework. Review capacity could been extra layers over the virtualized system[10]the Mainly their quality ought to be evaluated.

ii. Event: - The state changed and other factor of system availability.

iii. Log: - Comprehensive information about users.

iv. Monitoring :- It should be prevented from unauthorized intrusive attacks and it should be limited to the providers need for particular.

4. Conclusion

As we evaluated in this paper, these are loads of favourable position in utilizing a cloud based framework, however there are parcel of issue in essentially execution which must be understood. Distributed computing is a problematic innovation. There are as yet a few issues exist in administrations show, for information security, accessibility and honesty. Putting away the information in remote server prompts some security issue. Many investigations have been led to find the issue that influences privacy, review, and control of information to discover an answer for them. These arrangements will prompt more secure distributed storage which will likewise prompt more acknowledgments from the general population and the trust on the cloud will increment.

5.References

[1] Kartik Kumar & Yung hsiang LU, "cloud computing for mobile users",ieee,2010pp51-56

[2] P. Mell and T. Grance, "The NIST Definition of Cloud Computing, "NIST, Special Publication 800145, Sep. 2011

[3] Z. Zhou and D. Huang, "Efficient and secure data storage operations for mobile cloud computing,"inProceedings of the 8th International Conference on Network and Service Management. International Federation for Information Processing, 2012, pp.37–45.

[4] M. Lori, "Data security in world of cloud computing," Co-published by the IEEE Computer And reliability Societies, pp. 61–64, 2009.

[5] C. Wang, K. Ren, W. Lou,J. Li," Toward publicly auditable secure cloud data storage services," Network, IEEE, vol. 24, no. 4, pp. 19–24, 2010.6]

[6] A. Donald and L. Arockiam, "A secure authentication scheme for mobi cloud," in Computer Communication and Informatics (ICCCI), 2015 International Conference on, Jan 2015, pp. 1–6.

[7] C. Wang, Q. Wang, K. Ren, and W.Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in INFOCOM, 2010Proceedings IEEE. Ieee, 2010, pp. 1–9.

[8] K.Yang and X.Jia "Data storage auditing service in cloud computing:challenges, methods and opportunities," World Wide Web, vol.15, no. 4, pp. 409–428, 2012.

[9] S. Subashini, V. Kavitha " A Survey on security issue in service delivery models of cloud computing", pp. 1-11,2011

[10] Flavio Lombardi, Roberto Di Pietro " Secure virtualization for cloud computing". Elsevier, pp.1113- 1122,2011.

[11] M.T. Khorshed, A.S. Ali, " A survey on gaps,threats ,remidition , challenges and some thoughts for proactive action in cloud computing", vol 28,pp 833-851,2012

[12] W Baker"M" 2011 DBIR [online]availablewww.wired.com/images/threatlevel/2011/04/DBIR.pdf

[13] Wei-tekTsai, Xinsun, Balasooriya "Service oriented Cloud computing Architecture" ieee, pp.684-689.2010

[14] Zetta,"Zetta:enterprises cloud storage on demand", http://www/zetta.net/2006

[15] M. Sookhak, H. Talebian, E.Ahmed, A. Gani, and M. K. Khan, "A review on remote data auditing in single cloud server: Taxonomy and open issues," Journal of Network and Computer Applications, vol. 43,pp. 121–141, 2014.

[16] X. Wang, B. Wang, and J. Huang, "Cloud computing and its key techniques," in Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on, vol. 2. IEEE, 2011, pp. 404 –410.

[17] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013.]

[18] Z. Qiao, S. Liang, S. Davis, and H. Jiang, "Survey of attribute based encryption," in Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2014 15th IEEE/ACIS International Conference on, June 2014, pp. 1–6.

[19] Shashi, Anuranjan Mishra "Cloud computimg models: background ,data security & security issue" IJSECA Vol 1,2017.

[20] S. Ramgovind, M. M. Eloff, and E. Smith, "The management of security in cloud computing," in Information Security for South Africa (ISSA), 2010. IEEE, 2010