CLOUD SECURITY RESEARCH- A COMPREHENSIVE SURVEY

Sunita Swain and Rajesh Kumar Tiwari

ABSTRACT

Cloud computing is a new computing paradigm that delivers computing resources as a set of reliable and scalable internet-based services allowing customers to remotely run and manage the services. It is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud Computing is an abstraction based on the idea of pooling physical resources and presenting them as virtual resources. It is indeed a novel model for provisioning resources, staging applications, and platform independent consumer access to services. The major concern of the use of Cloud services is security because many attackers constantly try to take advantage of vulnerabilities in mobile networks to access data stored in the remote cloud servers. Certifying the security of cloud computing is a major task in the cloud computing environment. This paper summarizes a number of peer-reviewed articles on security threats in cloud computing and the preventive methods. The objective of our research is to understand the cloud components, security issues, and risks, along with emerging solutions that may potentially mitigate the vulnerabilities in the cloud.

Index Terms *Cloud Computing, Cloud Security, Security Threats, Virtualization, Service Level Agreement, Cloud Provider, Cloud Carrier*

Reference to this paper should be made as follows:

Sunita Swain and Rajesh Kumar Tiwari, (2020), "Cloud Security Research- A Comprehensive Survey" Int. J. of Electronics Engineering and Applications, Vol. 8, No. 2, pp. 29-39, DOI-10.30696/IJEEA.VIII.II.2020.29.39

Biographical notes:

Sunita Swain *is Asst Professor in R. V. S. College of Engineering and Technology, Jamshedpur. She is pursuing her PhD from ISM IIT Dhanbad, India.*

Dr. Rajesh Kumar Tiwari *is Professor and Dean of Academic Affairs, R.V.S. College of Engineering and Technology, Jamshedpur, Jharkhand. He has completed his PhD form BIT Mesra Ranchi. His research interest includes Data Security, Cloud Computing, Machine Learning and Database Management System. He has Published more than fifty research papers in reputed International Journals.*

I. INTRODUCTION

Cloud computing is rapidly becoming a significant service in the Internet computing[1] . Cloud-based computing services have grown in popularity in recent years which bring great advantages to all kinds of computing activities including business support[2]. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction(NIST Cloud Computing definition) . It is a deliberation dependent on pooling physical resources and introducing them as virtual resources. Cloud computing is increasingly being adapted by a wide range of users starting from commercial entities to consumers. It is indeed a novel model for provisioning resources, staging applications, and platform independent consumer access to services.Because of its adaptable foundation , netcentric approach and ease of access ,the cloud computing has turned out to be pervasive. Its far reaching utilization is anyway being reduced by the fact that the cloud computing paradigm is yet helpless to address security issues which may thus irritate the nature of administration as well as the protection of customers'data[3].

This paper comprises of various security issues in cloud computing, different types of risks, vulnerabilities, and potential controls in cloud computing. It also provides information on the cloud architecture and framework. Moreover, this paper identifies potential future research areas related to security in cloud computing. The paper is organized as follows: The cloud architecture is discussed in section 2. Section 3 discusses the security implication in deployment model.Different security issues in cloud computing and its controls are explained in section 4. Finally, section 5 concludes the paper with potential future directions.

II.NIST CLOUD COMPUTING REFERENCE ARCHITECURE

Fig 1 shows the reference architecture. The Architectural Components of the Reference Architecture describes the important aspects of service deployment and service orchestration. The overall service management of the cloud is acknowledged as an important element in the scheme of the architecture.

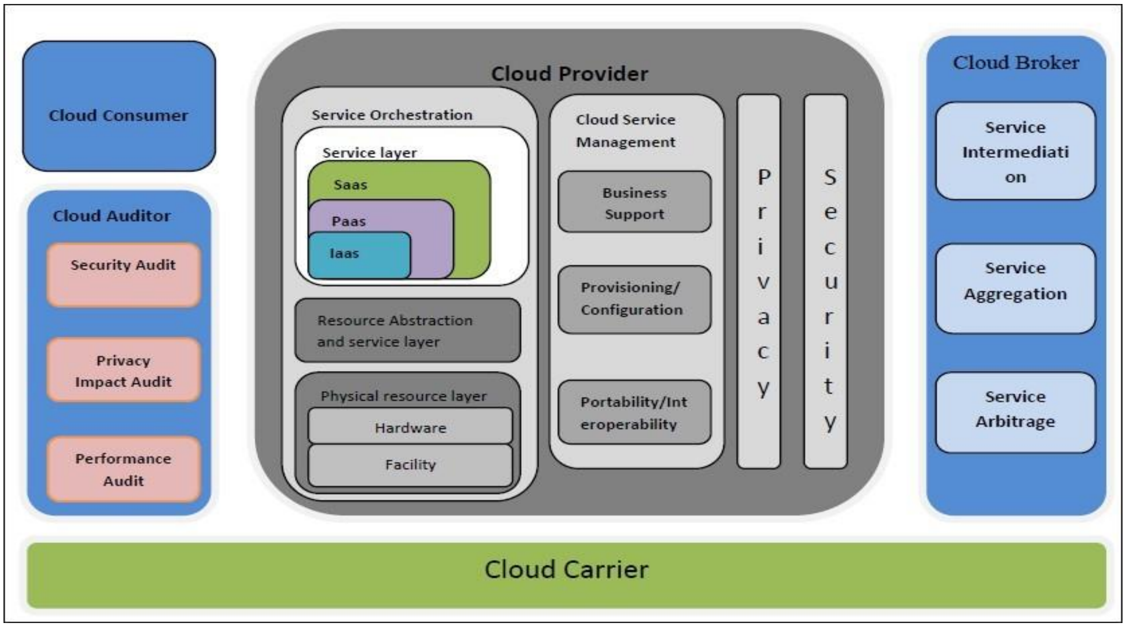

FIG 1:-NIST Cloud Computing Architecture

The Overview of the Reference Architecture describes five major actors with their roles & responsibilities using the newly developed Cloud Computing Taxonomy. The five major participating actors are the Cloud Consumer, Cloud Provider, Cloud Broker, Cloud Auditor and Cloud Carrier. These core individuals have key roles in the realm of cloud computing.

Table 1 -Actors in Cloud Computing

Actor	Definitio n
Cloud Consumer	A person or organization that maintains a business relationship with, and uses service from, Cloud Providers.
Cloud Provider	A person, organization, or entity responsible for making a service available to interested parties.
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
Cloud Broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers.

III. SECURITY IMPLICATION ON CLOUD DELIVERY MODEL

The types of service models that have emerged under cloud computing technology are Software-as-a- Service (SaaS), Platform-as-aService (PaaS), and Infrastructure-as-a-Service(IaaS)[4].

Table 2-Cloud Delivery Model

Delivery Type	Description	Responsibility	Security Threats
IaaS (Infrastrucure as a Service)	In this service, computing resources such as processing, storage and networks can be provisioned**.**	IaaS have access to virtual computers, network-accessible storage, network infrastructure components, and other fundamental computing resources on which they can deploy and run arbitrary software.	VM security – securing the VM operating systems and workloads from common security threats that affect traditional physical servers, such as malware and viruses, using traditional or cloud- oriented security solutions.[5]
PaaS (Platform as a Service)	The infrastructure is controlled by the cloud service provider but is different in that the users can deploy their software	PaaS can employ the tools and execution resources provided by cloud providers to develop, test, deploy and manage the applications hosted in a cloud environment	SOA related security issues – the PaaS model is based on the Service-oriented Architecture (SOA) model. This leads to inheriting all security issues that exist in the SOA domain such as DOS attacks, Man-in-the-middle attacks, XML- related attacks, Replay attacks, Dictionary attacks, Injection attacks and input validation related attacks [6, 7].

SaaS (Software as a Service)	In this service, the cloud service provider provides software and the cloud infrastructure to the clients .	In SaaS the cloud provider deploys, configures, maintains and updates the operation of the software applications on a cloud infrastructure so that the services are provisioned at the expected service levels to cloud consumers.	In the SaaS model enforcing and maintaining security is a shared responsibility among the cloud providers and service providers (software vendors). The SaaS model inherits the security issues like data security management [8] (data locality, integrity, segregation, access, confidentiality, backups) and network security.

IV. CLOUD SECURITY ISSUES

In this section, work is mainly focusing on several categorized security issues and their solutions. First, the work displays a short presentation about security issue in cloud computing at that point exhibits their answers. A security issue is something occurring in any assets attacks, mis-configuration, fault, damage, escape clauses, and shortcoming in the framework [9]. There is much difference between cloud specific issue and general issue. The cloud related issue is produced because of the qualities of distributed computing, defined by NIST and it is significantly more difficult to execute security arrangements in cloud condition. Cloud is a set of technology, process, people, and commercial construct. Like all other technology, process, people, and commercial construct, cloud too has vulnerabilities [10]. Some of the open issues and threats that needs urgent attention.

The survey categorized security issue in different parts as data storage and computing security issues, virtualization security issues, Internet and services related security issues, network security issues, access control issues, software security issues, trust management issues, and compliance and legal issues[11] . The introduced data storage and computing issues, virtualization and stage related issues are going under the cloud delivery models. Furthermore, the study going on Internet related issues. At last, the study covers security issues identified with trust and legal issues.

1) Data storage and computing security issues

Data is a fundamental piece of cloud computing. Data put away in the cloud is secluded and vague to the clients. In the remote storage or third party storage, the fundamental issue is that the client does not realize what occur after the capacity of the data in the cloud [12]. The data owner does not aware of the locality of the data in the cloud, security administrations and security systems utilized for securing the cloud information. The nature of administration is the imperative angle in the distributed storage. A cloud storage provider needs a legitimate method and systems to store efficiently and unwavering quality information in the cloud. The client information is put away in the cloud server farms. Numerous enormous players give distributed storage at extremely shabby focused cost. This disseminated information is profoundly excess and put away at different physical areas. The electrical source excess and efficient cooling guarantee that the information is exceedingly accessible. By the assistance of legitimate space allotment component, cloud space can be reused efficiently [13]. The information excess gives a system in which information is backed up to another cloud server for guaranteeing high accessibility of information. If there should arise an occurrence of one server farm is totally disappointment, supplier utilize reinforcement information server.

Cryptographic mechanisms are utilized to secure the cloud data and information. It is a straight forward thought to accomplish the security of the cloud. It changes over plain text information into another form called cipher text. The thought in view of the presumption that it is unfeasible to compute the estimation of the plain content information; if figure content is accessible [13]. So, they require carefully and strong implementation of cryptography methods because the whole security depends upon the key that is used as an encryption key.

2) Virtualization security issues

The purpose for the wide reception of cloud computing in the business is the virtualized cloud computing. Improvement of cloud benefit for business reason, cloud supplier require trust on VM [14]. In the cloud conditions, the virtualization is the essential prerequisites of any administration. The multi-tenure and virtualization idea gives more profit, yet this idea is not free from dangers and assaults. Numerous assailants perform co-area assault to get to the administrations. Step by step individuals do look into in this field to accomplish legitimate sensible and virtual segregation.

3) Internet and services related security issues

The cloud Infrastructure is created with many administrations and assets, as well as required a transporter that is transmitting the information between sender and recipient. The Internet is a bearer; transmit the substantial number of bundles from source to goal as advanced information. The information is gone through various hubs, so it is not sheltered. Because of an acquired issue with the Web 2.0 numerous new sorts of dangers developed. The Internet abuses numerous security issues like MitM attacks, IP spoofing, port scanning, malware injections, and packet sniffing. The cloud services is accessed and managed over the web and standard web browser that is not a safe solution for the end users. There are numerous security arrangements are accessible yet individuals accept that exchanged information through the Internet is not safe.

4) Network security issues

The network is the fundamental part of the cloud computing. In this way, issues are not just present in the VM, administration, or application level, yet additionally alive in the network level. The system level issues can specifically affect the cloud framework [14]. The cloud arrange nature is dynamic, so the issue is viewed as both internal and external systems. Any client can play out a

DoS attack to affect the accessibility of the administration. This can likewise affect the system data transmission and increase the congestion in the network.

5) Access control issues

The access control security refers to the protection from unauthorized read/write permissions. The access security is kept up by verification with blend of an Email ID or username and secret key. In the multi-occupant cloud condition have a substantial number of clients [12]. Every client can access cloud services utilizing sites or front-end interface. The web innovation or sites are an attack entryway. In this way, individuals require some access control mechanism. To solve this issue, it is important to separate and provide different authorization to every part either logical or physical from one another.

6) Software security issues

Software security is the very concerning point in the present circumstance. These days, individuals write each software in own thoughts and utilize different programming languages, such programming languages have thousand or a large number of lines of code. Along these lines, that is the reason individuals unable to measure the software security in the system. Even developer follows the set of rule and constraint, a single bug can be counter a security problem.

7) Trust management issues

Trust is a non-quantifiable parameter in cloud computing. It must be available in the middle of the client and the cloud provider for outsource their business and information. What's more, the trust likewise identified with the resources those are utilized, including storage device, web based access, computational algorithms, virtualization mechanisms, and so on. There are many explanations behind an unsuccessful trust built up between two parties [7]. The trust plays an important role for any system.

8) Compliance and legal security issues

The Service Level Agreement is a document plays an important role in the cloud business model. It contains an agreement between the two communicating parties, all service related information, and terms and conditions of the service [12]. The SLA is signed by the both parties to show they agree with this agreement.

9) Data storage and computing security issues

Data is a fundamental piece of cloud computing. Data put away in the cloud is secluded and vague to the clients. In the remote storage or third party storage, the fundamental issue is that the client does not realize what occur after the capacity of the data in the cloud [12]. The data owner does not aware of the locality of the data in the cloud, security administrations and security systems utilized for securing the cloud information. The nature of administration is the imperative angle in the distributed storage. A cloud storage provider needs a legitimate method and systems to store efficiently and unwavering quality information in the cloud. The client information is put away in the cloud server farms. Numerous enormous players give distributed storage at extremely shabby focused cost. This disseminated information is profoundly excess and put away at different physical areas. The electrical source excess and efficient cooling guarantee that the information is exceedingly accessible. By the assistance of legitimate space allotment component, cloud space can be reused efficiently [13]. The information excess gives a system in which information is backed up to another cloud server for guaranteeing high accessibility of information. If there should arise an occurrence of one server farm is totally disappointment, supplier utilize reinforcement information server.

Cryptographic mechanisms are utilized to secure the cloud data and information. It is a straight forward thought to accomplish the security of the cloud. It changes over plain text information into another form called cipher text. The thought in view of the presumption that it is unfeasible to compute the estimation of the plain content information; if figure content is accessible [13]. So, they require carefully and strong implementation of cryptography methods because the whole security depends upon the key that is used as an encryption key.

10) Virtualization security issues

The purpose for the wide reception of cloud computing in the business is the virtualized cloud computing. Improvement of cloud benefit for business reason, cloud supplier require trust on VM [14]. In the cloud conditions, the virtualization is the essential prerequisites of any administration. The multi-tenure and virtualization idea gives more profit, yet this idea is not free from dangers and assaults. Numerous assailants perform co-area assault to get to the administrations. Step by step individuals do look into in this field to accomplish legitimate sensible and virtual segregation.

11) Internet and services related security issues

The cloud Infrastructure is created with many administrations and assets, as well as required a transporter that is transmitting the information between sender and recipient. The Internet is a bearer; transmit the substantial number of bundles from source to goal as advanced information. The information is gone through various hubs, so it is not sheltered. Because of an acquired issue with the Web 2.0 numerous new sorts of dangers developed. The Internet abuses numerous security issues like MitM attacks, IP spoofing, port scanning, malware injections, and packet sniffing. The cloud services is accessed and managed over the web and standard web browser that is not a safe solution for the end users. There are numerous security arrangements are accessible yet individuals accept that exchanged information through the Internet is not safe.

12) Network security issues

The network is the fundamental part of the cloud computing. In this way, issues are not just present in the VM, administration, or application level, yet additionally alive in the network level. The system level issues can specifically affect the cloud framework [14]. The cloud arrange nature is dynamic, so the issue is viewed as both internal and external systems. Any client can play out a

DoS attack to affect the accessibility of the administration. This can likewise affect the system data transmission and increase the congestion in the network.

13) Access control issues

The access control security refers to the protection from unauthorized read/write permissions. The access security is kept up by verification with blend of an Email ID or username and secret key. In the multi-occupant cloud condition have a substantial number of clients [12]. Every client can access cloud services utilizing sites or front-end interface. The web innovation or sites are an attack entryway. In this way, individuals require some access control mechanism. To solve this issue, it is important to separate and provide different authorization to every part either logical or physical from one another.

14) Software security issues

Software security is the very concerning point in the present circumstance. These days, individuals write each software in own thoughts and utilize different programming languages, such programming languages have thousand or a large number of lines of code. Along these lines, that is the reason individuals unable to measure the software security in the system. Even developer follows the set of rule and constraint, a single bug can be counter a security problem.

15) Trust management issues

Trust is a non-quantifiable parameter in cloud computing. It must be available in the middle of the client and the cloud provider for outsource their business and information. What's more, the trust likewise identified with the resources those are utilized, including storage device, web based access, computational algorithms, virtualization mechanisms, and so on. There are many explanations behind an unsuccessful trust built up between two parties [7]. The trust plays an important role for any system.

16) Compliance and legal security issues

The Service Level Agreement is a document plays an important role in the cloud business model. It contains an agreement between the two communicating parties, all service related information, and terms and conditions of the service [12]. The SLA is signed by the both parties to show they agree with this agreement.

V. CONCLUSION

The cloud computing model is one of the promising computing models for the service providers, cloud providers and cloud consumers. This paper provides a comprehensive view on cloud computing research over the years. The various security issues in communication ,security and privacy, computational and Service Level Agreement and power efficiency are explored .During computation both virtualization and data related security issues are considered to be the most vulnerable entity. Virtualization is the fundamental component of cloud computing and expands its estimation. Currently security has a ton of last details which frightens off a great deal of potential clients. Every element in the cloud should be analyzed at the macro and micro level and an integrated solution must be designed and deployed. In the cloud consumer, provider, broker, carrier, auditor and everyone else has to take the necessary precautions against risk to secure the cloud-computing platform.

REFERENCES

[1] Manvi,S.S.,Krishna Shyam , G.,2014,Resource management for Infrastructure as a service (Iaas) in cloud computing:a survey.J.Netw. Computer Appl. 41(May), 424-440.

[2] Chang, V.Walters, R.J.,Wills, G.B., 2016. Organisational sustainability modelling – an emerging service and analytics model for evaluating cloud computing adoption with two case studies. Int. J.Inf. Manag 36 , 167-179.

[3] Review A survey of security issues for cloud computing Minhaj Ahmad Khan Bahauddin Zakariya University Multan,Pakistan. Journal of Network and Computer Applications71 (2016) 11– 29.ELSEVIER

[4] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583–592.

[5] An Analysis of the Cloud Computing Security Problem Mohamed Al Morsy, John Grundy and Ingo Müller. 2010 Asia Pacific Cloud Workshop, Colocated with APSEC2010, Australia.

[6] Meiko Jensen, Jörg Schwenk, Nils Gruschka and Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing," in IEEE ICCC, Bangalore 2009, pp. 109- 116.

[7] Z. Wenjun, "Integrated Security Framework for Secure Web Services," in IITSI 2010, pp. 178-183.

[8] S. Subashini, ,Kavitha, V., "A survey on security issues in service delivery models of cloudcomputing," Journal of Network and Computer Applications, vol. In Press, Corrected Proof.

[9] Ashish Singh , Kakali Chatterjee. Cloud security issues and challenges: A survey, Journal of Network and Computer Applications 79 , Elsevier (2017).88-115.

[10] A Comprehensive Survey on Security in Cloud Computing Gururaj Ramachandra, Mohsin Iftikhar Farrukh Aslam Khan, The 3rd International Workshop on Cyber Security and Digital Investigation (CSDI 2017). Procedia Computer Science 110(2017) 465–472.

[11] .Mu-Hsing Kuo, Opportunities and challenges of cloud computing to improve healthcare services. J.Med, Internet Res. (2011).

[12] Anitha Y1 1Department of Computer Science and Engineering, Punjab Technical University 1SSCET, Pathankot, India. Security Issues in Cloud Computing - A Review.International Journal of Thesis Projects and Dessertations(IJTPD) Vol-1,Issue-1,p-1-6.Oct-Dec-2013.

[13] Mojtaba Alzadeh,Saeid Abolfazli,Mazdak Zarari,Sabariah Baharun,Kouichi Sakurai, Authentication in mobie cloud computing:A Survey. Journal of Network and Computer Applications 61 .Elsevier (2016), 59-88.

[14] Amani S. Ibrahim, James Hamlyn-Harris and John Grundy, Computer Science & Software Engineering, Faculty of Information & Communication Technologies Swinburne University of Technology, Hawthorn Vicyoria, Australia, Emerging Security Challenges of Cloud Virtual Infrastructure, In Proceedings of APSEC 2010.

[15] L.FB Soares, D. AB Fernandes, J.V. Gomes, M.M. Freire, P. RM Inácio, Cloud security: state of the art, in: Security, Privacy and Trust in Cloud Systems, Springer, Berlin, Heidelberg, 2014, pp. 3–44.