ISSN (Online): 2455-7838
SJIF Impact Factor (2017): 5.705

EPRA International Journal of

Research & Development

(IJRD)

Monthly Peer Reviewed & Indexed International Online Journal

Volume: 3, Issue:11,November 2018

Published By :
EPRA Journals

SJIF Impact Factor: 5.705 Volume: 3 | Issue: 11 | November | 2018 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)

A STUDY ON CLOUD ARCHITECTURE AND SECURITY ISSUES

T.K Bhoi[1]
[1]IEEE Member

A. K. Pradhan[2]
[2]IEEE Member

ABSTRACT

Cloud computing is a computational model with the help of which a user or an organization can have various computing services and infrastructure available to him. It provides an efficient and seamless connectivity to the various resources such as data, software, hardware, databases, servers, compilers etc to the user that can be used as per the needs and requirements. In cloud Computing, direct hardware are not needed. In spite of all services cloud data security is a big challenge to us in present scenario.

KEY WORDS: *Cloud security, public cloud, private cloud, privacy risks, Security Challenges.*

I. INTRODUCTION

The growing popularity of cloud computing services is a crucial driver behind converting it into a viable business proposal for reducing the cost of both infrastructure and operations, thus it has become to efficiently manage security and privacy risks in the cloud environment as well as iron out legal issues related to it [1],[2],[3]. In this study, security issues related to cloud computing are discussed along with legal steps undertaken to mitigate such issues. The main motivation behind this study is growing demand for cloud services that are capable, cost effective and secure (Sen, no date). As every organization is constantly searching for new methods of increasing revenue return and decreasing cost, So cloud computing platform is a technological development[4].

II. CLOUD ARCHITECTURE

Computing Building Blocks

1) *Deployment models*

Depends on the various uses of the cloud. Consists of hybrid, community, private and public cloud.

a) Private Cloud

Utilized by an establishment and its individuals. Framework is claimed by a specific establishment and it might be taken care of by the organization or a middle person. Just an organization and its individuals may have section to serve on a particular private cloud.

Example: Eucalyptus System

b) Public Cloud

Used by the public. Mainly based on pay-per-use model and it caters a self- service model. It is less secured compared to other cloud models because the data is available to the public and hence more prone to attacks[5].

Example: Microsoft Azure

c) Community Cloud

Used by a group of users who have the same objective. The infrastructure is shared by multiple institutions and is handled by them or a mediator[6],[7].

Example: Facebook

d) Hybrid Cloud

Utilizes the properties of one of the above considered models. It is outfitted as a sole unit and limited by an ensured organize. This model cooks more control of the information [8], [9].

e) Delivery Models

The cloud provides its services in different form. They can be infrastructure, platform and services. There are some expensive applications like CRM, ERP etc.

2. Hallmarks of cloud

Provides the services on demand and hence need not pay in advance. These services are available on all smart devices.

3. Service Models

There are three different models. They are:

a). Software as a service (SAAS)

It is the highest layer which gives an entire application. This empowers the client to take out the way toward building and dealing with the application all alone gadgets. SAAS vendors are in charge of overseeing and sending the framework and procedures required to run the full arrangement[10],[11], [12], [13].

b) Platform as a service (PAAS)

PAAS gives a stage and arrangement stack. Gives a framework abnormal state of coordination, chiefly to execute and test cloud applications. Example: Google App Engine

c) Infrastructure as a service (IAAS)

Administrations are executed by sharing equipment assets. The primary goal is to make assets available by applications and working framework [14], [15].
Example: Amazon S3

III. CLOUD COMPUTING CHARACTERISTICS

On Demand self-service: A cloud might individually attain computing possibilities, as per the use of different servers, network storing, as on request, without communicating with cloud provider.
Broad Network Access: Services are delivered across the Internet within a standard mechanism and access to the services is possible through assorted customer tools.

Resource pooling: A multitudinous model is employed to serve different types of clients by making pools of different computing resources, as per the request of customers these have different resources which can be assigned and reassigneddynamically[10],[11].

Rapid Elasticity: Capabilities might be elastically provisioned or rapidly released. From customers view, the provided possibilities come out to be limitless and must have the capability to purchase in any quantity at any time.

Measured Services: The provision procured by different clients is measurable. The use of asset will be directed, estimated, and accused for contributor and asset [12], [13].

IV. CLOUD SECURITY CHALLENGES

These are some of the challenges that are needed for security and their knowledge is necessary for mitigation purposes.

Authentication: Throughout the internet data stored by cloud user is available to all unauthorized people. Henceforth the certified user and assistance cloud must have interchangeability administration entity.

Access Control: To check and promote only legalized users, cloud must have right access control policies. Such services must be adjustable, well planned, and their allocation is overseeing conveniently. The approach governor provision must be integrated on the basis of Service Level Agreement (SLA) [14], [15].

Policy Integration: There are many cloud providers such as Amazon, Google which are accessed by end users. Minimum number of conflicts between their policies because they user their own policies and approaches.
Service Management: In this different cloud providers such as Amazon, Google, comprise together to build a new composed services to meet their customers need. At this stage there should be procure divider to get the easiest localized services [16], [17].

Trust Management: The trust management approach must be developed as cloud environment is service provider and it should include trust negotiation factor between both parties such as user and provider. For example, to release their services provider must have little bit trust on user and users have same trust on provider [18], [19].

Privileged User Access:

Any client that accesses data outside the enterprise then the user has to take permission or buy membership for prevention of data leak.

Data Location:

The client shouldn't know where the data is stored or the place form where the data is being propagated (hosted).

Availability:

Data should be available everywhere even when the range of company is not available at that moment. This is called anywhere-anytime availability of software.

Regulatory Compliance:

The hosting providers should never allow external audits or allow installation of external new security certificates.

Recovery:

If under any condition the data is ruined by any disaster, man-made or natural, the providers should be able to deliver the backup data to the users on time.

Security Risks in Cloud Computing

Cloud Computing helps us to access data and information for particular organization. Hackers and Attackers have found out loopholes to gain access to these information.

IP Spoofing:

Fig 5 Showing IP Spoofing attack by modifying packets

IP Spoofing is known as analysis of the data that is being sent over the network. When data is sent over the network the attacker manipulates the data. The manipulation is done in a way that the IP address of the trusted system and then modifies the packet information and then sends it to the receiving system [16], [17].

DDOS attack:

In this attack, DDOS the attacker spoofs the information and sends many requests of the data.

Insecure Interface:

Interface is the model that helps the client to adhere to the cloud internal software. Management of data, identity management, monitor service and other functions that happen on the cloud are done through these interfaces. If interface is not secure, then data theft is very easy [20], [21].

Malicious Insider:

The insiders such as the employees or any user can manipulate the data, such that they can even sell the information to other organizations. Any this causes severe data leaks in cloud computing.

Data Loss or Leakage:

There are two process taking place when data is being transmitted from host to client. First of all, data is being stored in a far of place and secondly, data transmission happens from one mode of execution to modes that are multiple in nature. Thus, if any modification happen in between, the loss or leakage of data occurs

Malware attack on VM:

Cloud Security can be compromised by the unwanted Vm-based virus or tool-kits that are used to cloak the information sent to the server by the user. Same process can happen when the data is being sent form the server to the client. These viruses or malwares are also used to store the data such as registry information, system logs, and security program details. This flow charts shows us how these risks are interrelated [18], [19].

But security & privacy issues caused by hackers and crackers and many security researchers have concluded that due to loss of control, invalid storage, access control and data boundary. The cloud computing is insecure and many preventive measures have been implemented over the time to reduce such risks.

DoS attacks:

One cannot stop the denial of service attacks because it is not possible one can mitigate the e ect of these attacks but cannot stop these attacks. DoS assaults overpower resources of a cloud service so clients can't get to information or applications. Politically roused assaults get the front features, however programmers are similarly prone to dispatch DoS assaults for pernicious goal including extortion. What's more, when the DoS assault happens in a distributed computing condition, process burn charges experience the roo op. e cloud supplier ought to invert the charges, yet consulting over what was an assault and what wasn't will take extra time and irritation. Most cloud suppliers are set up to deny DoS assaults, which takes consistent observing and moment alleviation [22], [23].

System vulnerabilities

Vulnerabilities of the system are exploitable program bugs in the OS that programmers intentionally use to control or invade a PC framework. Fortunately, essential IT cleanliness goes far towards shielding you from this sort of genuine assault. Since machines exist in your cloud supplier's server farms, be sure that your supplier hones normal weakness examining alongside convenient security xes and overhauls.

***Written security policies plan*:**

If the cloud service providers have a written security plan of policies then the security of the data will be guaranteed, if the cloud service provider do not have a security policies written plan then the cloud is not safe and security of the data cannot be guaranteed as they do not have a written plan of security policies. is means that their data security program development. Organizations that have not formalized their security strategies cannot be trusted with your touchy corporate/ client information. Strategies shape the system and establishment and without security is just an idea in retrospect [20], [21].

Multifactor authentication

If the cloud providers provide the multifactor authentication for example one time password and mobile [3] code then the security of the data will be more tight as it will be protected by multi factors. If someone try to unlock the data through password one time wrong password will be sent to the data owner at his or her mobile so that he can authenticate the login to the data [17]. Multifactor authentication make the level of protection of data more high.

Access to data:

Data of enterprise must be accessed and seen by the administration not by the users. is access will provide the enhance security to the data over the cloud. Many cloud applications are equipped towards client collaboration, however free programming trials and join openings open cloud administrations to pernicious clients. A few genuine assault sorts can ride in on a download or sign in DoS attacks, email spam, computerized click extortion, and pilfered substance are only a couple of them. Your cloud supplier is in charge of solid episode reaction structures to distinguish and remediate this wellspring of assault. IT is in charge of checking the quality of that structure and for observing their own cloud condition for manhandle of resources[22], [23].

Organizational Security Management:

Existing security management and information secu- rity life-cycle models signi cantly change when en- terprises adopt cloud computing. In particular, shared governance can become a signi

cant issue if not prop- erly addressed. Despite the potential bene ts of using clouds, it might mean less coordination among di er- ent communities of interest within client organiza- tions. Dependence on external entities can also raise fears about timely responses to security incidents and implementing systematic business continuity and di- saster recovery plans. Similarly, risk and cost-bene t issues will need to involve external parties. Customers consequently need to consider newer risks introduced by a perimeter-less environment, such as data leakage within multi-tenant clouds and resiliency issues such as their provider's economic instability and local disasters

Similarly, the possibility of an insider threat is sig- ni cantly extended when outsourcing data and pro- cesses to clouds. Within multi-tenant environments, one tenant could be a highly targeted attack victim, which could signi cantly a ect the other tenants. Ex- isting life-cycle models, risk analysis and management processes, penetration testing, and service attestation must be reevaluated to ensure that clients can enjoy the potential bene ts of clouds.

The information security area has faced signi cant problems in establishing appropriate security metrics for consistent and realistic measurements that help risk as- sessment. We must reevaluate best practices and develop

According to Recent researches, by the end of 2013 there will be more than 10 thousand mobile applications that will be executed through cloud computing. That traction will push the revenue of mobile cloud computing to $5.2 billion.

V. CONCLUSION

Here in this paper we have provided an overview of cloud computing its definitions, constituting elements (that are cloud platform and cloud applications) and finally we have discussed about the challenges of implementing cloud computing in mobile applications and their possible solutions. In future , we will concentrate about the security in IOT based Cloud Environment.

REFERENCES

1. *Tarun Dhar Diwan, Durga Chandrakar, Implementation Of Android Based Mobile Phone Search Engine And Live Image Sender, International Research Journal Of Engineering And Technology, Volume: 02 Issue: 03, ISSN: 2395- 0056, June-2015*
2. *A. Wood, L. Fang, J. Stankovic, and T. He, SIGF: A Family of Configurable Secure Routing Protocols for Wireless Sensor Networks, ACM Security of Ad Hoc and Sensor Networks, Best Paper Award, October 31, 2006.*
3. *S. Munir, J. Stankovic, C. Liang, and S. Lin, New Cyber Physical System Challenges for Human-in-the-Loop Control, 8th International Workshop on Feedback Computing, June 2013.*
4. *Somayya Madakam , R. Ramaswamy , Siddharth Tripathi, 'Internet of Things (IoT): A Literature Review' , Journal of Computer and Communications , 2015, 3, 164 -173 Published Online May 201 5 in Sci Res .*
5. *http://www.scirp.org/journal/jcc*
6. *Alok Kulkar et al, / (IJCSIT), Healthcare applications of the Internet of Things: A Review , International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014, 6229-6232*
7. *Andrea Zanella, Internet of Things for Smart Cities, IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 1, FEBRUARY 2014, pp 22-32*
8. *J. P. Lynch and J. L. Kenneth, "A summary review of wireless sensors and sensor networks f or structural health monitoring," Shock and Vibration Digest, vol. 38, no. 2, pp. 91– 130, 2006*
9. *T. Nuortio, J. Kytöjoki, H. Niska, and O. Bräysy, "Improved route planning and scheduling of waste collection andtransport," Expert Syst. Appl., vol. 30, no. 2, pp. 223– 232, Feb. 2006.*
10. *B. Jana and J. Poray, "A performance analysis on elliptic curve cryptography in network security," 2016 International Conference on Computer, Electrical & Communication Engineering (ICCECE), Kolkata, 2016, pp. 1-7.doi:10.1109/ICCECE.2016.8009587*
11. *S. Mitra, B. Jana and J. Poray, "A novel scheme to detect and remove black hole attack in cognitive radio vehicular ad hoc networks(CR-VANETs)," 2016 International Conference on Computer, Electrical & Communication Engineering (ICCECE), Kolkata, 2016, pp. 1-5. doi: 10.1109/ICCECE.2016.8009589*
12. *B. Jana, S. Mitra and J. Poray, "An analysis of security threats and countermeasures in VANET," 2016 International Conference on Computer, Electrical & Communication Engineering (ICCECE), Kolkata, 2016, pp. 1-6. doi: 10.1109/ICCECE.2016.8009588*
13. *S. Mitra, B. Jana, S. Bhattacharya, P. Pal and J. Poray, "Quantum cryptography: Overview, security issues and future challenges," 2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix), Kolkata, 2017, pp. 1-7. doi:10.1109/OPTRONIX.2017.8350006*
14. *B. Jana, J. Poray, T. Mandal and M. Kule, "A multilevel encryption technique in cloud security," 2017 7th International Conference on Communication Systems and Network Technologies (CSNT), Nagpur, 2017, pp. 220-224.doi: 10.1109/CSNT.2017.8418541*
15. *Jana B., Poray J. (2018) A Hybrid Task Scheduling Approach Based on Genetic Algorithm and Particle Swarm Optimization Technique in Cloud Environment. In: Bhateja V., Coello Coello C., Satapathy S., Pattnaik P. (eds) Intelligent Engineering Informatics. Advances in Intelligent Systems and Computing, vol 695. Springer, Singapore*
16. *Jana B., Chakraborty M., Mandal T. (2019) A Task Scheduling Technique Based on Particle Swarm Optimization Algorithm in Cloud Environment. In: Ray K., Sharma T., Rawat S., Saini R., Bandyopadhyay A. (eds) Soft Computing: Theories and Applications. Advances in Intelligent Systems and Computing, vol 742. Springer, Singapore*
17. *Jana, Bappaditya and Chakraborty, Moumita and Mandal, Tamoghna and Kule, Malay, An Overview on Security Issues in Modern Cryptographic Techniques (May 4, 2018). Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2018 held at Malaviya National Institute of Technology, Jaipur (India) on March 26-27, 2018. Available at SSRN: https://ssrn.com/abstract=3173527 or http://dx.doi.org/10.2139/ssrn.3173527*
18. *Jana B., Poray J. (2016) VANET: OVERVIEW, SECURITY ISSUES AND CHALLENGES,*

International Journal of Engineering Research-Online, Vol-4, Issue-2, Pages-451-459, http://www.ijoer.in

19. *M Chakraborty B. Jana, T. Mandal and M. Kule, " An Performance Analysis of RSA Scheme Using Artificial Neural Network " 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)), Bengaluru, 2018, dOI: 10.1109/ICCCNT.2018.8494032*
20. *Mandal, Tamoghna and Jana, Bappaditya and Mitra, Saptarshi and Poray, Jayanta, A Study on Risk Assessment in Information Security (October 5, 2018). Available at SSRN: https://ssrn.com/abstract=3261593 or http://dx.doi.org/10.2139/ssrn.3261593*
21. *M Chakraborty B. Jana, T. Mandal and M. Kule, " An Performance Analysis of RSA Scheme Using Artificial Neural Network " 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)), Bengaluru, 2018, dOI: 10.1109/ICCCNT.2018.8494032*
22. *M. Chakraborty, B. Jana, T. Mandal and M. Kule, "An Performance Analysis of RSA Scheme Using Artificial Neural Network," 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bangalore, 2018, pp. 1-5. doi:10.1109/ICCCNT.2018.8494032*
23. *S. Mitra, B. Jana and J. Poray, "Implementation of a Novel Security Technique Using Triple DES in Cashless Transaction," 2017 International Conference on Computer, Electrical & Communication Engineering (ICCECE), Kolkata, India, 2017, pp. 1-6.doi: a10.1109/ICCECE.2017.8526233*