A Systematic Review on Cloud Computing Security Issues

[1]Azra Zia Ansari, Research Scholar, Department of Computer Science & Engineering, Integral University, Lucknow, India,

[2]Mrs. Kavita Agarwal, Associate Professor, Department of Computer Science & Engineering, Integral University, Lucknow, India

Abstract

Cloud computing is an approach to manage limitations or include restrains progressively without setting resources into new structure , preparing new work force or favoring new programming. As information exchange is a noteworthy activity in the current life, information security ends up being a significant issue. Before separating the security issues, the significance of distributed or cloud based processing is discussed and the analysis of various issues related to cloud based security has also been done. The security issues identified with cloud computing has been investigated here and a local adaptable security solution for the cloud has been proposed. This paper also looks at the cloud security issues in terms of features like ease of adaptability, access, etc. This work is expected to empower scientists and experts to think about various security threats and work on finding out their effective solutions.

Keywords: *Cloud Computing, Security threats, Cloud Architecture*

I Background

Since the last decade, cloud computing is seen as an intriguing issue in scholarly zones, attributable to the inherent qualities of the system, by which, we could watch the entire world in an astounding perspective, and specialists of a lot of zones, e. g., worldwide vitality emergency, environmental change, heath care,etc [4]benefited from this. Moreover, the improvement of cloud faces the bottleneck, which is brought about by its own exceptionally low security power, low calculation ability and low correspondence capacity. What's more terrible, in some specific situations, for instance, information protection is that it exceptionally asked to get detecting secure information progressively, which was practically unthinkable for little size endeavors that utilized their own frameworks [8].

Consequently, the cloud computing rose as another star in scholastic and business areas. As Cloud processing may get omnipresent in future, various analysts considered the likelihood of joining new subject with distributed computing to take care of the issues which are infer-able from the extraordinary property of issues. Indeed, the blend defeats a few difficulties, for example, stockpiling issues and openness. The on-request benefits trademark that cloud administrations provide, is a significant property to most little estimate undertakings who have constrained asset. In any case, vulnerabilities despite everything exist, particularly in security issues.

For some, it is a perspective that allows ease in handling of resources while for others, it is just a way to deal with programming and accessing the data from the cloud [10]. Cloud computing is well known in association and scholarly nowadays since it gives its clients adaptability and accessibility of information. Moreover cloud computing lessens the cost by enabling the sharing of data to the affiliation. Affiliation can port their data on the cloud with the objective that their financial specialists can use their data. In any case, Cloud gives distinctive office and points of interest yet simultaneously it has a couple of issues related to safe access and limit of data. A couple of issues are there related to cloud security like seller lock-in, multi-tenure, diminished control, interruption of administration, loss of information and so on. The prime concern is to consider various types of methods to make sure about the cloud model.

The cloud computing has expanded wide contemplation, yet there are various security and privacy related issues of appropriated processing have kept the associations from totally enduring cloud stages. The security scenes of dispersed registering occur as frequently as conceivable in some acclaimed associations, for instance, Microsoft, Amazon, Google and other market player. Generally, the security system data is guaranteed by the customers by applying some security strategies, tools and best practices such as including firewall which is similar to the IDS [3]. In any case, the condition is totally extraordinary in distributed computing which is depicted in figure 1.Everything, such as software , hardware, and application data are passed on and taken care of in respective cloud domains. Mosley customer are unaware with the security procedure opted by the companies. Along these lines, there is an uncertainty among customers and cloud suppliers.

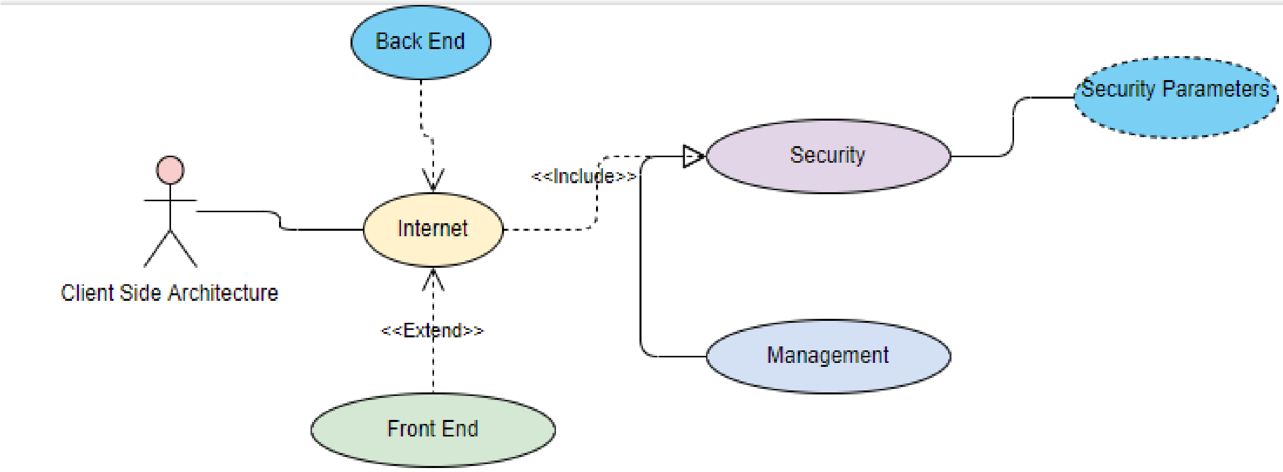

Figure 1 Cloud Computing with security issues

II Related Work

In the span of last few years the concept of cloud has emerged in two broad perspectives – renting of infrastructure on cloud, or renting any utility on cloud. Where the former one deals with the hardware and software utilization, the latter one is restricted to availing various utilities and not the hardware from the cloud service and infrastructure providers [13]. As the cloud based computation evolved with time, the computing world has been presented with various wordings like Software, Platform and Infrastructure as a Service, popularly known as SaaS, PaaS and IaaS. As per previous discussion, the 'cloud computing' is a concept, and so are its terminologies that define various amalgamations of cloud computing.

Cloud Computing Security issues have been focused by few organizations. The Cloud Security Alliance is a nonprofit organization formed to promote the use of best practices for giving security affirmation inside Cloud Computing, and give instruction on the employments of Cloud Computing to help secure every single type of computing. The Open Security Architecture is another organization focusing on security issues [5]. They have proposed the open security architecture pattern, which is an endeavor to delineate center cloud works, the key jobs for oversight and hazard moderation, collaboration across various internal organizations, and Controls that require additional control. For example, certification, accreditation and safety assessment series is significantly increased in order to ensure that the operation is being done to another provider "outsourced". Securing the System and Services is pivotal to guarantee that the procurement of administrations is overseen effectively. Possibility arranging assists with guaranteeing a way of how to react in case of interferences to support conveyance. Figure 2 demonstrates the elevated level perspective on the distributed computing security by the experts.

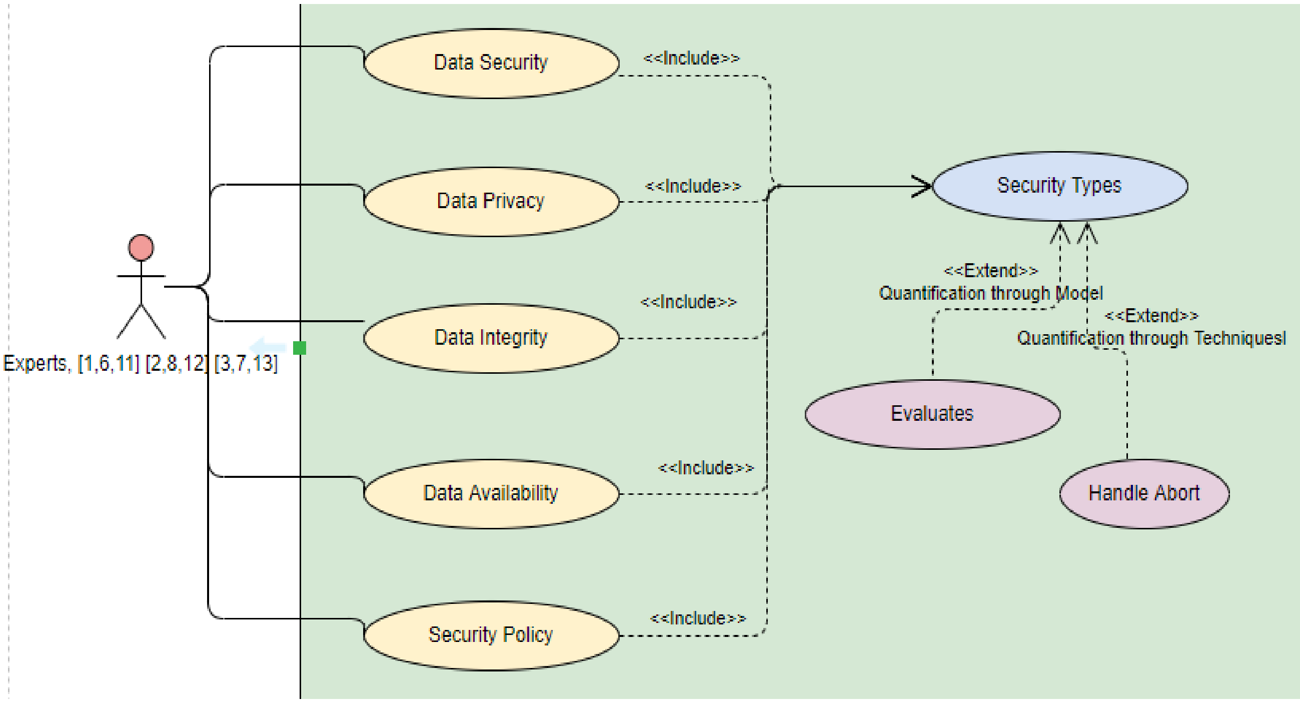

Figure 2 Highlighted issues of cloud computing by experts

Cloud computing comes with numerous possibilities and challenges simultaneously. Of the challenges, security is considered as a crucial hindrance for cloud computing in its evolution as a technology **(A. Kundu et. al., 2010).** The security challenges for cloud computing have a wide range and they are also evolving on real time basis. Data location is a crucial factor in cloud computing security. Location transparency is one of the conspicuous adaptabilities for cloud computing, which is a security danger simultaneously – without knowing the particular area of information stockpiling, the arrangement of information insurance represent some district may be seriously influenced and disregarded. Cloud clients' very own information security is along these lines, a critical worry in a cloud computing environment **(G. Thippa Reddy et. al.)**. While providing data security for customers' personal or business related data by only applying the simple strategic policies or specifically applying alone technical security is insufficient to deal with all type of security issues to maintain the high quality of service (L. Wang et. al., 2008).

Another factor that acts as a detrimental factor in acceptance of usage of cloud organization is integrity or trust (Hyseni et. al., 2019). This is because it directly related to the authenticity, Authorization, and accessibility of the cloud pro associations. Establishing trust or integrity may transform into the best approach to develop a compelling cloud based computing system. The course of action of trust model is fundamental in cloud computing because it's an intriguing region for every stakeholder for any given cloud computing scenario. In context to the cloud, the trust depends on several features like computer assisted management, procedures and approaches **(P. Anand, 2016).**

Table 1 Contribution table by Experts with Year

Experts	**Year**	**Contribution**	**Methodology**
L. Wang et. al.	2008	A study on cloud computing	Theocratically
R. Maggiani et. al.	2009	Cloud computing is discussed with communication	Theocratically
A. Kunduet. al.	2010	Introduced new services	Method based
Akhil Behl et. al	2011	Emerging Security Challenges in Cloud Computing	Evolutions
Gonzalezet. al.	2012	Current security concerns and solutions for cloud computing	Quantitative analysis
V. Inukolluet. al.	2014	A study on security issues associated with Big Data	Theocratically
G. Thippa Reddyet. al.	2015	Framework for Cloud security	Validated

P. Anandet. al.	2016	Threat Assessment	Quantitative Assessment
D. H. Adnaan Arbaaz Ahmedet. al.	2018	Study of Security Issues and Research Challenges	Evaluation
Hyseniet. al.	2019	Proposed a model related to cloud security	Quantification

III Critical Observations

After effective study and completion of the precise survey of the available scholarly works, some significant basic perceptions are there which mentioned below in a point wise manner.

1.Chances are that we upgrade the cloud computing at initial phase of security process which in turn will enormously support the cloud framework and will also be helpful to the customer.

2. The inclusion of more highlights and functionalities, for example, factors related to security, risk factors and schedule factors in the cloud environment at different phase of security will have positive impact in the pursuit of reducing the risk.

2. The security factors influencing the cloud framework have to be distinguished and afterward the arrangement of variables, which are important in context to the information security should be concluded.

3. Further, initializing and quantifying the security at cloud environment is also important.

IV Conclusion

Cloud computing is another rising development, which every affiliation these days customize so as to support the adaptability of their relationship in information dissemination, trade. This empowers them to overhaul their benefit, interoperability, limit, and adaptability. Despite numerous advantages in computational environment of the cloud, there are few security related issues which could cause nonappearance of security and trust for data and customers assurance, progressive inaction, organizational loss , and sketchy nature of service provider's consistence. The security issue has been ended up being extra intricate in various cloud based model as new paradigm have appeared into the most troublesome degree identified with the model's data security and the customers' assurance arrangement. The security issue ended up being extra intricate under the cloud model as new expansions have appeared into the troublesome degree identified with the model’s data security, customers' assurance mastermind security, along with the stage and establishment issues. This work was performed on basic level study to feature the computational security issues of cloud. The finding of this assessment underlines that there are certain standard issues related with computational execution of cloud which are security factors, cloud environment, data validation and data efficiency. These issues form a basis of research in the field of cloud computing so as to remove the void created by the security issues . This void may be addressed by giving either a particular technique or definite model to reduce these points of concern.

References

1. L. Wang, Gregor Laszewski, Marcel Kunze and Jie Tao, "Cloud Computing: A Prespective Study", *New Generation Computing-Advances of Distributed Information Processing*, vol. 28, no. 2, pp. 137-146, 2008.
2. R. Maggiani, "Communication Consultant Solari communication Cloud computing is changing How we communicate", *IEEE International Professional Conference IPCC*, pp. 1-4, July 2009, ISBN 1-42444357-4.
3. A. Kundu, C. D. Banerjee, P. Saha, “Introducing New Services in Cloud Computing Environment”, International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.
4. Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, “On technical Security Issues in Cloud Computing,” Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

5. B. R. Kandukuri, R. V. Paturi and A. Rakshit, “Cloud Security Issues,” 2009 IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009. In Proceedings of IEEE SCC'2009. pp. 517-520, 2009. ISBN: 978-0-7695-3811-2
6. Ronald L. Krutz, Russell Dean Vines “Cloud Security A Comprehensive Guide to Secure Cloud Computing”, Wiley Publishing, Inc.,2010.
7. Xuan Zhang, Nattapong Wuwong, Hao Li, etc. Information security risk management framework for the cloud computing environments. In Proc. Of 10th international conference on computer and informaiton technology, 2010.
8. Special Publication 800-30. Guide for Conducting Risk Assessments. America: National Institute of Standards and Technology, 2011.
9. European Network and Information Security Agency (ENISA). Cloud Computing: Benefits, risks and recommendations for information security.2009.
10. Akhil Behl Emerging Security Challenges in Cloud Computing (An insight to Cloud security challenges and their mitigation) , 2011.
11. Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Naslund, M. and Pourzandi, M.. A quantitative analysis of current security concerns and solutions for cloud computing. Journal of Cloud Computing, 1(11), 1-18, (2012).
12. Hamlen, K., Kantarcioglu, M., Khan, L. and Thuraisingham, V. (2010). Security Issues for Cloud Computing. International Journal of Information Security and Privacy, 4(2), 39-51. doi: 10.4018/jisp.2010040103.
13. Youssef, A.E. (2012). Exploring Cloud Computing Services and Applications. Journal of Emerging Trends in Computing and Information Sciences, 3(6), 838-847.
14. Zissis, D and Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28, 583–592. doi:10.1016/j.future.2010.12.006.
15. D. H. Adnaan Arbaaz Ahmed, "Cloud Computing: Study of Security Issues And Research Challenges", International Journal of Advanced Research in Computer

Engineering & Technology (IJARCET), April 2018.

16. D. A. L. B. S. a. B. C. Hyseni, "The Proposed Model to Increase Security of Sensitive Data in Cloud Computing", *International Journal of Advanced Computer Science And Applications*, vol. 9, no. 2, pp. 203-210, 2019.

17. G. Thippa Reddy, K. Sudheer, K. Rajesh and K. Lakshmanna, "Emplolying Data Mining on Highly Secured Private Clouds for Implementing a Security – as a – Service Framework", Journal of Theoritical and Applied Information Technology, vol. 59, no. 2, 2015.

18. V. Inukollu, S. Arsi, and S. Ravuri, “Security Issues Associated with Big Data in Cloud Computing,” Int. J. Netw. Secur. Its Appl., vol. 6, no. 3, pp. 45–56, 2014.

19. P. Anand, J. Ryoo, H. Kim, and E. Kim, “Threat Assessment in the Cloud Environment – A Quantitative Approach for Security Pattern Selection,” in IMCOM ’16, 2016, p. 8.