International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

Cloud Computing Environment with Security Issues

Brijesh Kumar Bhardwaj

Abstract*: Security is a significant subject of a few software systems. Cloud computing continue to be assertion as a most important innovation in IT management. The objective of this paper is to make available the recent advancement and a wide impression of the obtainable literature cover an assortment of dimensions of the Cloud security. In addition to the efforts of the paper industry, it also concludes the directions created at various levels for future research in cloud security base on related work. This possibly will be extremely useful, predominantly for the entrance level researchers, who desire to behavior the research in these connected areas.

***Keywords* : Cloud Environment, Security Factors, Challenges**

I. INTRODUCTION

With the rapid enlargement as well as demand of Cloud computing, the most important concern is on its security along with privacy, which is unwavering by the policies, controls and technologies needed to defend the data, applications [2, 8]. In addition to the connected infrastructure of Cloud computing. These challenges inflict more than a few new research questions to the research group of people to make sure proper security of the IT infrastructure [6]. To develop secure cloud system is the contributory process of different steps in adding together to reflections of each phase is the substance of study to calculate the immediately right impact of cloud security. Security is an incessant process for every step-in cloud computing concept [7]. Security is a multi-attribute. Cloud security is in relation to sympathetic risk and how to manage them. A quantitative move toward be able to be a big amount data. In order to, conceptual technique to develop a technique which can assess the real level of security assessment. Security development techniques are tremendously desirable for internal structure of cloud, design and other feature of cloud [1]. Cloud computing is an original computing model that will intersect the large-scale compute resources to successfully put together, and to compute resources as a service to users.

II. BACKGROUND

To appreciate the basics of cloud computing and storing secure data in the cloud, has been involved for more resources.

Revised Manuscript Received on November 30, 2019.
***** Correspondence Author
Dr. Brijesh Kumar Bhardwaj*, Associate Professor, Department of MCA, Dr. R. M. L. Avadh University, Ayodhya, India

It provides an assessment of the literature to discuss a range of segment data protection aspects. H. Abbas et. al. Highlights the concept of cloud computing [1]. Some of the concepts are looking for examples of long-term applications in this paper, which is known to be urban how using cloud compute and they never give to hand the increasing world to benefit from the up-and-benefit Can Incoming technology.

On the other hand, Abdul Muthlib Khan [3] The data discussed the concerns of consumers regarding the move to the cloud. According to Chen and Zhao, is a security issue for their data to be sedentary large enterprises of the major reasons to move to the cloud. The authors have provided extraordinary analysis on the data as well as privacy issues fortification related to cloud security. In addition, he also talked about the available solutions to these issues [5].

III. LITERATURE REVIEW

In the past few decades different works have been done by various other experts in the field of cloud security:

Abdelhamid M. (2009) To enhance users' privacy had proposed a number of techniques based on the RSA algorithm. Author's main aim is to authorized users access to remotely stored data. To be saved with the authenticity of all the data.

S Subhashini and V Kavitha (2010), He proposed a good criterion for protection with the help of different techniques as well as providing various types of technical protection.

M. Ahmed et al. (2010) Expanded a range of security-related centralizations involving customers and cloud related resources. Securing data cloud resources and clients on cloud servers is their main objective.

V. Krishna Reddy and Dr. L. S. S. Reddy (2011), Proposed architecture of the different levels of cloud security. Securing data cloud resources and clients on cloud servers is their main objective. They Software as a Service (SaaS) such offer also studied different kind of services provided by the cloud servers, Platform as a Service (Paa) and Infrastructure as a Service (IaaS) ".

Syam Kumar P and Subramanian R (2011), Sobel sequence to protect customer data and their resources with the proposed elliptical Crolet cloud. It is used to provide security using certain rules and eliminate authenticity called accuracy of data. They also provide protection against various types of hackers on the Internet which can be harmful to our data.

Abbas Amina (2012) In his paper he used a good storage system primarily for cloud computing, in view of the secure objectives. use algorithms to increase with security while maintaining the accuracy of the data they used the RSA algorithm for it.

And another algorithm which they use the client data storage AES algorithm to maintain privacy

Sajjad Hashemi (2013) Several security related challenges are proposed for cloud data storage. A variety of suggestions have been made for cloud computing systems to improve data storage security and use algorithms to address problems or challenge security. For example, they use AES, DES.

Swarnalata Bollavarapu and Bharat Gupta (2014) Proposed cloud computing data storage system protection for data clients. The system RSA various algorithms for encryption and decryption techniques, RC4 and use of ECC.

R. Velumadhava Rao (2015) identifying the various data security challenges and solutions in cloud computing. The main objective of the practical test is to increase the security of data in order to maintain integrity.

Dr. Salim Ali Abbas, Amal Abdul Baqi Maryoosh (2015) Customer data and provide an effective, flexible and secure way to provide security to cloud resources. They data accuracy and provide Elliptic Curve Cryptography algorithm for security.

AL-Museelem Waleed, Li Chunlin (2016) Provided that the lack of security is affecting user data and cloud resources. UEC (Ubuntu Enterprise Cloud) is used to solve the privacy problem of authenticity. He used the algorithm, it is to encrypt and decrypt the data to ensure the confidentiality and integrity protection in the cloud [36].

Table 1 has now represented various researchers' works and scope of extension by various researchers:

TABLE 1 CONCISE THE VALUABLE COMMENTS BY EXPERTS

EXPERTS	YEAR	CONTRIBUTIONS	METHODOLOGY	SCOPE FOR EXTENSION
Li Yan [29]	2018	Address to cloud secure architecture	Crypto graphic concept	Data security and privacy can be addressed
Ashish Singh et. al [30]	2017	Discussed the issue of cloud security	DDoS mitigation terminology	Enhance the security of data storage in the cloud computing systems
Qusay Kanaan Kadhim [35]	2017	Highlighted the cloud computing security issues	Cloud Service Providers (CSPs) mechanisms	Attention to add the risk issues with fault at cloud level
Prachi Deshpande et. al [33]	2016	Risk factors in security and the service assurance in a Cloud environment	Theocratically Approaches	Move to validation concept
Mihir Manavati et. al [31]	2014	Provide the approach for Enhancement of cloud security	Used the Data base terminology for confidentiality, Integrity and availability	Provides the approaches for data security, authentication and verification
Abdul Muttalib Khan [3]	2015	Highlighted the comparative study on cloud security approaches	Multicloud Databases (MCDB), Homomor phic Encryption, SWAP model, Cryptogra phic Techniques	Move to encryption and decryption techniques
R. Kaur et. al [4]	2014	Explained the Algorithms about cloud	Some light on AES Algorithm, DES, RC5, DSA	Proposed the analysis model which based on cloud
Dinh, H.T [27]	2013	Expert evaluated the performance effect	Multiple-layer architecture, Prototype implementation	Researcher can move to data risk security evaluations
Nagarjuna [11]	2013	Developed the model for various segment at cloud level	Hyper-visor terminology	Experts can be virtualization and distributed storage techniques for cloud environment with security
Ainul Azila Che Fauzi et. al [32]	2012	Provides the protection criteria about the cloud computing	RSA Algorithms based observations	Empirical validation for cloud computing environment

Lombardi F et. al [7]	2011	Provide the visualization concept for cloud security	Used the approaches Cloud Protection System (ACPS)	Experts can be developing the new algorithms for cloud efficiency
R. L Grossman et. al [9]	2010	Explained the cloud computing services	Parallel Computing techniques over Clouds	Focused on methodological, and empirical evaluation
Vieira K [34]	2010	Provide secure speech and text encryption Mechanism	Captcha Breaking	Produce the new methodology for intruder may spam and over exhaust the network resources

Such as the requirement arises security factors were documented and collected for their function in cloud environment. Cloud security opinion is attainable from side to side the help of finding new security factors which in a straight line and indirectly affect security features of cloud. Cloud security is associated by way of free significant security pillar which can be expediently to the point by the acronym CIA (confidentiality, integrity, availability). Cloud security challenges assessment is within reach with the assist of judgment innovative security factor which directly as well as not directly have an effect on the security features of cloud environment as well as presented at Table 2. Cloud security factors are presented at figure 1.

3.1 Confidentiality at Cloud Level Confidentiality refers to the prevention of the unauthorized access of the data and hence making sure that only the user who has the permission can access the data [21]. This is one of the important features of security. In this paper, we do a study of the security factors related to cloud computing and also discuss that confidentiality is vital for cloud data, enhance the confidentiality and thus ensuring the cloud security. User privacy is very user hides the identity when he receives data or manipulates it [23, 10]. Cloud database access patterns and record customized database for a particular user is assured of access Privacy on keeping secret. While ensuring privacy, some additional aspects are considered important. User privacy and access to privacy. [13, 33]

3.2 Integrity at Cloud Level

This section also addresses the issues of data stored in the data integrity verification and privacy protection in the cloud servers that use Abiswasit third party to verify the integrity of the data stored in the cloud server [22]. The significance of the work lies in the detection of any tampering with the customer data and the ability to maintain the confidentiality of data during the integrity verification process, which prevents the customer's data in exchange for any damage or loose [26]. Cloud data integrity verification and a critical need to address privacy protection issues in the area. Presented in order to provide verification data integrity in cloud computing has focused on ways where data integrity.

3.3 Availability at Cloud Level

Service availability in the cloud user's perspective and response time are two important safeguards. Such performance measure is the amount required to set up and modeling them appropriately; the model should include parameters in large numbers, while still tractable [24]. Exact availability to guarantee the security services for cloud users and performance analysis are critical requirements. The data that ensures availability is available to trusted users and systems when they access the authorized manner database [25]. It is the degree or extent that is calculated in terms of database operations is payable, which reliability.

Fig 1 Basics security parameters for cloud

Table 2 Commonly accepted security factors on cloud environment by various Experts

SECURITY FACTORS FOR CLOUD →	Confidentiality	Integrity	Availability	Authorization	Reliability	Authentication

EXPERTS / RESEARCHERS ↓						
Li Yan (2018) [29]	√	√	√	√	√	√
M. B. Mollah (2017) [18]	√	√	√	√		√
K. Jakimoski (2016) [15]	√	√	√	√	√	
Abdul Muttalib Khan (2015) [3]	√	√		√	√	√
Yunchuan Su et. al (2014) [12]		√	√	√	√	√
H. Rasheed (2014) [19]	√	√	√			√
Dinh, H.T (2013) [27]	√	√	√	√	√	√
M. Alhomidi (2013) [20]	√	√	√	√	√	
A. N. Khan (2013) [16]	√		√	√	√	√
Doukas, C (2012) [28]	√	√	√	√	√	√
D. Zissis (2012) [39]	√	√	√	√		√
Olislaegers (2012) [40]	√	√		√	√	√
D. Huang (2011) [37]	√		√	√	√	√
A. M.-H. Kuo (2011) [17]	√	√		√		√
Z. Zhou (2011) [38]						
Krešimir Popović (2010) [14]	√	√	√	√	√	√

IV. RESEARCH CHALLENGES

Cloud computing security addresses the challenge of security at private, public and hybrid level cloud computing architectures and also the challenges of allow applications in addition to development platforms in security perspective. Various existing issues contain not been fully addressed to security, at the same time as new challenges maintain up-and-coming from industry applications. Some of the question is raised to challenging cloud security in following manner.

1. What are the challenges that directly influence cloud security?
2. Is there any standard cloud security architecture?
3. Is any quantitative approach for cloud security?
4. Can we enhance the cloud data security?
5. Can we develop any approach with targeting to Cloud security?

V. SUGGESTIONS

After successful completion of the systematic literature review some important critical observation are as follows. If we enhance the security at cloud stage may greatly supports to system and as well as help to cloud based environment.

1. In order to add more features and functionalities such as security factors in cloud at various stages of effective security environment which have positive impact on data security.
2. A security factors affecting to secure cloud system must be identified and then the set of factors relevant at the cloud should be finalized.
3. Further, the no of affecting factors must be selected in cloud security then matching with the appropriate order.

VI. CONCLUSION

Cloud computing has immense prospects, but with equivalent number of security threats. One of the main security doubts with the cloud computing model is the multi-tenancy. Various measures addressing to cloud security are also explored. Cloud computing can be secured only if the enhanced the security level. The paper aim at constructing a proper model of the present state of affairs and future forecast of Cloud security. Cloud security has to be critically reviewed with major importance. Researcher's surveys cloud security approaches that verify authenticity of cloud data. These approaches have been illustrated as a review for ensuring the long-term Confidentiality, integrity and availability of data stored at remote un trusted hosts. In this survey, we analyze several of security approaches,

compare them with respect to expected cloud security guarantees and discuss their limitations. In future, it is planned develop the Framework for enhance the cloud security using internal policy.

REFERENCES

1. H. Abbas, O. Maennel, S. Assar, "Security and privacy issues in cloud computing", Institut Mines-Télécom and Springer-Verlag France, (2017).
2. B. Duncan, M. Whittington (2016), "Enhancing Cloud Security and Privacy: The Power and the Weakness of the Audit Trail", CLOUD COMPUTING: *The Seventh International Conference on Cloud Computing, GRIDs, and Virtualization*,.
3. Abdul Muttalib Khan , Dr. Shish Ahmad , Mohd. Haroon, "A Comparative Study of Trends in Security in Cloud Computing", Fifth International Conference on Communication Systems and Network Technologies, IEEE (2015).
4. R. Kaur ,S. Kinger, "Analysis of Security Algorithms in Cloud Computing", international Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 3, March (2014).
5. Casola, V., Cuomo, A., Rak, M. and Villano, U., "The Cloud Grid approach: Security analysis and performance evaluation", Future Generation Computer Systems, 29, 387-401, (2013).
6. Chen D and Zhao H, "Data Security and Privacy Protection Issues in Cloud Computing," International Conference on Computer Science and Electronics Engineering, Hangzhou, pp. 647-651, (2012).
7. Lombardi F, Pietro R.D, Secure virtualization for cloud computing, In Journal of Network and Computer Applications, Volume 34, Issue 4, (2011).
8. Shahin Fatima, "SECURITY ISSUES IN CLOUD COMPUTING: A SURVEY", IJARCS, (2018).
9. R. L Grossman, "The Case for Cloud Computing", IT Professional, Vol. 11(2), 23-27, (2009).
10. Teneyuca, D, "Internet cloud security: The illusion of inclusion", Information Security Technical Report, 16, 102-107, (2011).
11. Nagarjuna, Kalyan Srinivas, S.Sajida, Lokesh, "Security Techniques for Multitenancy Applications in Cloud", International Journal of Computer Science and Mobile Computing, Vol.2 Issue. 8, 248-251, 2013.
12. Yunchuan Su, "Data Security and Privacy in Cloud Computing", International Journal of Distributed Sensor Networks, (2014).
13. Kashif Munir and Prof Dr. Sellapan Palaniappan," Framework for Secure Cloud Computing ", International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.3, No.2, April (2013).
14. Krešimir Popović, Željko Hocenski,"Cloud computing security issues and challenges", MIPRO, May 24-28, Opatija, Croatia (2010).
15. K. Jakimoski, "Security Techniques for Protecting Data in Cloud Computing," Int. J. Grid Distrib. Comput., vol. 9, no. 1, pp. 49–56, (2016).
16. A. N. Khan, M. L. Mat Kiah, S. U. Khan, and S. A. Madani, "Towards secure mobile cloud computing: A survey," Futur. Gener. Comput. Syst., vol. 29, no. 5, pp. 1278–1299, (2013).
17. A. M.-H. Kuo, "Opportunities and Challenges of Cloud Computing to Improve Health Care Services," J. Med. Internet Res., vol. 13, no. 3, p. e67, (2011).
18. M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," Journal of Network and Computer Applications, vol. 84. pp. 38–54, (2017).
19. H. Rasheed, "Data and infrastructure security auditing in cloud computing environments," Int. J. Inf. Manage., vol. 34, no. 3, pp. 364–368, (2014).
20. M. Alhomidi and M. Reed, "Security Risk Analysis as a Service," in 2013 8th International Conference for Internet Technology and Secured Transactions, ICITST, pp. 156– 161, (2013).
21. Ateniese, G., et al., Provable data possession at untrusted stores, in Proceedings of the 14th ACM conference on Computer and communications security, ACM: Alexandria, Virginia, USA. p. 598-609, (2007).
22. Erway, C., et al., Dynamic provable data possession, in Proceedings of the 16th ACM conference on Computer and communications security, ACM: Chicago, Illinois, USA. p. 213-222, (2009).
23. Shen, Y., Li, K., Yang, L.T., "Advanced Topics in Cloud Computing" Journal of Network and Computer Applications 12, Springer, 301–310 (2010).
24. Casola, V., Mazzeo, A., Mazzocca, N., Victoriana, V, "A Security Metric for Public key Infrastructures", Journal of Computer Security, Springer, 15(2), 78–85 (2007).
25. Sharma, P., Sood, S.K., Kaur, S.: Security Issues in Cloud Computing. In: Mantri, A., Nandi, S., Kumar, G., Kumar, S. (eds.) HPAGC. CCIS, vol. 169, pp. 36–45. Springer, Heidelberg (2011).
26. Jamil, D., Zaki, H.:, "Cloud Computing Security", International Journal of Engineering Science and Technology 3(4), 3478–3483 (2011).
27. Dinh, H.T.; Lee, C.; Niyato, D.; Wang, P.: A survey of mobile cloud computing: architecture, applications, and approaches. Wirel. Commun. Mob. Comput. 13(18), 1587–1611 (2013).
28. Doukas, C.; Maglogiannis, I.: Bringing iot and cloud computing towards pervasive healthcare. In: Proceedings of the Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp. 922–926. IEEE, Palermo, Italy (2012).
29. Li Yan, "Cloud Computing Security and Privacy", Proceedings of the International Conference on Big Data and Computing, ACM, Pages 119-123, (2018).
30. Ashish Singh et. al. "Cloud security issues and challenges: a survey", Journal of Network and Computer Applications, (2017).
31. Mihir Manavati, Cloud Security: A Gathering Storm", ACM, (2017).
32. Ainul Azila Che Fauzi. Et.al., "On Cloud Computing Security Issues", Springer-Verlag Berlin Heidelberg (2012).
33. Prachi Deshpande et. al., "Security and service assurance issues in Cloud environment", The Society for Reliability Engineering, Quality and Operations Management (SREQOM), Springer, (2016).
34. Vieira K, Schulter A, Westphall C, Westphall C,"Intrusion detection techniques for Grid and Cloud computing environment", IT Prof 12(4):38–43, (2011).
35. Qusay Kanaan Kadhim et.al., "A Review Study on Cloud Computing Issues", International Conference on Big Data and Cloud Computing (ICoBiC) (2017).
36. A. N. Khan, M. L. Mat Kiah, S. U. Khan, and S. A. Madani, "Towards secure mobile cloud computing: A survey," Futur. Gener. Comput. Syst., vol. 29, no. 5, pp. 1278–1299, (2013).
37. D. Huang, Z. Zhou, L. Xu, T. Xing, Y. Zhong, Secure data processing framework for mobilecloud computing, in: Proc. IEEE INFOCOM Workshop on Cloud Computing, INFOCOM '11, Shanghai, China, June (2011).
38. Z. Zhou, D. Huang, "Efficient and secure data storage operations for mobile cloud computing", IACR Cryptology ePrint Archive: 185, (2011).
39. D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Generation Computer Systems 28 (3) 583–592, (2012).
40. Anshul Mishra, Devendra Agarwal, MH Khan, "Confidentiality Estimation Model: Fault Perspective", International Journal of Advanced Research in Computer Science, Vol 8, Issue 5, May, 2017.

AUTHORS PROFILE

Dr. Brijesh Kumar Bhardwaj is Associate Professor in the Department of MCA, Dr. R. M. L. Avadh University Ayodhya India. He obtained his M.C.A degree from Dr. R. M. L. Avadh University Faizabad (2003) and M.Tech. in Computer Science and Engineering from K.N.I.T. Sultanpur and obtained Ph.D degree. His area of research is Software Engineering and Data Mining. Dr. Bhardwaj published numerous articles, several papers in refereed journals and conferences.