International Journal of Scientific Modern Research and Technology
(Volume: 01, Issue: 01, Number: 06) Paper ID: IJSMRT-20100106
ISSN: 2582-8150

Security Issues in Cloud Computing: A Perspective View

Mr. Deepak Kumar
PG Scholar
Dept. of CSE, MITS, Bhopal

Abstract- Cloud enlisting goes with different possible results and troubles simultaneously. Of the troubles, security is seen as an essential hindrance for dispersed registering in its manner to advance. The security challenges for dispersed figuring approach are genuinely amazing and monstrous. Data territory is a huge factor in disseminated processing security. Region straightforwardness is one of the obvious adaptabilities for dispersed processing, which is a security peril all the while – without knowing the specific region of data amassing, the plan of data protection speak to some district might be genuinely impacted and dismissed. Cloud customers singular data security is appropriately a crucial concern in a dispersed figuring atmosphere. To the extent customers individual or business data security, the fundamental systems of the cloud providers are of most raised monstrosity as the particular security only isn't agreeable to address the issue. Trust is another troublesome which raises security stresses to use cloud organization for the clarification that it is direct related to the legitimacy and authenticity of the cloud expert associations. Trust establishment may transform into the best approach to develop a productive conveyed registering atmosphere. The game plan of trust model is essential in dispersed registering as this is a run of the mill interest area for all accomplices for some arbitrary disseminated figuring circumstance. Trust in cloud might be dependent upon different factors among which some are computerization the heads, human parts, cycles and techniques. Trust in cloud is unquestionably not a particular security issue, yet it is the most convincing fragile factor that is driven by security issues normal in appropriated registering by and large. A wide scope of attacks that are applicable to a PC association and the data in transit also applies to cloud based organizations – a couple of risks in this class are man-in-the-middle attack, phishing, snooping, sniffing and other similar attacks. DDoS (Distributed Denial of Service) attack is one fundamental yet huge attack for dispersed processing establishment. The eminent DDoS attack can be an imaginable issue for disseminated processing, anyway not with any uncommon instance of having no way out to direct this.
Keywords: Cloud Computing, data storage, security.

I. INTRODUCTION

Progressing enhancements in the field of could figuring have colossally changed the strategy for enrolling similarly as preparing resources. In a cloud based figuring establishment, the resources are consistently in someone else's explanation or network and got to indirectly by the cloud customers. Taking care of is done remotely gathering the way that the data and various parts from an individual should be shipped off the cloud establishment or laborer for getting ready; and the yield is unending gracefully of required taking care of. Sometimes, it might be required or if nothing else plausible for a person to store data on inaccessible cloud laborers. These gives the going with three sensitive states or circumstances that are of explicit concern inside the operational setting of dispersed figuring:

• The transmission of individual fragile data to the cloud specialist,

• The transmission of data from the cloud specialist to clients' PCs and

• The limit of clients' own special data in cloud laborers which are far away specialist not guaranteed by the clients.

All the more than three states of dispersed processing are genuinely disposed to security break that makes the assessment and assessment inside the security parts of appropriated figuring practice a fundamental one.

There have been different blends that are being used in dispersed processing area, anyway the middle thought remain same – the structure, or for the most

 ISSN: 2582-8150

part, the resources remain somewhere else with someone else's ownership and the customers 'rent' it for the time they use the establishment. On occasion, taken care of tricky data at far away cloud laborers are moreover to be counted. Security has been at the focal point of safe enrolling practices. Exactly when it is attainable for any bothersome get-together to 'sneak' on any private PCs by techniques for different strategies for 'hacking'; the game plan of stretching out the expansion to get to someone's own special data by strategies for disseminated processing finally raises further security concerns. Appropriated processing can't discard this enlarged augmentation in view of its demeanor and approach. Consequently, security has reliably been an issue with conveyed processing practices.

II. BACKGROUND

Poorvika Singh Negi et. al, 2020, With the fast development in the amount of customers, there is a rising in issues related to gear disillusionment, web encouraging, space and memory assignment of data, which is clearly or by suggestion provoking the insufficiency of data. With the objective of offering kinds of help that are trustworthy, snappy and low in cost, we go to disseminated figuring practices. With a goliath improvement in this development, there is genuinely extending plausibility of its security being subverted by harmful customers. A way to deal with divert malicious traffic from systems is by using Honeypot.

Yang Ming et. al, 2019, Vehicular extraordinarily named associations (VANETs) are a growing huge perspective for unbelievably improving road system capability and traffic security. To for the most part send VANETs, in reality, it is essential to deal with the security and insurance issues in VANETs. In the proposed plot, a roadside unit (RSU) can at the same time affirm a great deal of got messages with the ultimate objective that the total affirmation time may be unequivocally lessened. Furthermore, the security examination exhibits that the proposed plot is provably secure in the discretionary prophet model and fulfill all the essentials on security and assurance.

Feifei Wang et. al, 2019, Nowadays, far off customer affirmation show expects an uncommon capacity in ensuring the security of data transmission and guaranteeing the insurance of customers for various association organizations. In this assessment, we discover two starting late introduced baffling affirmation plans are not as secure as they ensured, by demonstrating they experience the evil impacts of separated mystery key estimating attack, de-synchronization attack, meeting key disclosure attack, failure to achieve customer haziness, or forward secret. Furthermore, we reveal two atmosphere express confirmation plans have weaknesses like emulate attack.

Yicheng Yu et. al, 2019, The fuse of Internet of things (IoT) and circulated processing development has made our life more profitable starting late. Assisting conveyed processing, Internet of things can give more gainful and valuable organizations. People can recognize IoT organizations by methods for cloud laborers at whatever point and wherever in the IoT-based circulated processing atmosphere. Regardless, a great deal of possible association attacks bargain the security of customers and cloud laborers. To complete feasible access control and secure correspondence in the IoT-based conveyed processing atmosphere, character approval is key. In 2016, He et al. put forth a strange affirmation plot, which relies upon lopsided cryptography. It is ensured that their arrangement is good for withstanding a wide scope of known attacks and has incredible execution.

Xiaoying Jia et. al, 2019, Mobile edge preparing (MEC) licenses one to beat different limitations trademark in appropriated registering, in spite of the way that achieving the broad extent of security necessities in MEC settings stays testing. In this paper, we revolve around achieving imparted affirmation to mystery and un-conspicuousness, as this is basic in ensuring data security and customer insurance. Specifically, we plan a character based obscure confirmed key course of action show for the MEC atmosphere. The proposed show achieves normal affirmation in a single message exchange round, similarly as ensures both customer anonymity and un-detectability.

 ISSN: 2582-8150

Hamza Hammami et. al, 2019, Cloud figuring addresses the latest advancement that has transformed the universe of business. It is a promising course of action giving associations the possibility of remotely taking care of their data and getting to organizations at whatever point they are required and at a lower cost. In any case, re-appropriating IT resources in like manner brings dangers, especially for tricky information with respect to security and insurance, since all data and resources set aside in the cloud are regulated and compelled by cloud expert communities. On the other hand, cloud customers may need cloud expert centers not to comprehend what organizations being gotten to and how oftentimes they are using them. Thusly, arranging segments to make sure about assurance is a huge test. One promising investigation district is by methods for check instruments, which has pulled in various investigators in this delicate subject. For this, couple of courses of action have been devised and disseminated starting late to deal with this issue.

III. COMPARATIVE STUDY

Table 1: Comparative Study of different methods

SN	Authors	Title	Method	Outcome
1	Poorvika et.al	Intrution Detection and Prevention using Honeypot Network for Cloud Security	Honeypot Protocol	Reduce attack rate
2	Yang et.al	Efficient Certificate less Conditional Privacy-Preserving Authentication Scheme in VANETs	CPPAP (Conditional Privacy-Preserving Authentication Protocol)	Reduce communication cost
3	Feifei Wang et. al	Secure and Efficient ECC-Based Anonymous Authentication Protocol	ECC based AAP	Low throughput
4	Yicheng et. al	A Secure Authentication and Key Agreement Scheme for IoT-Based Cloud Computing Environment	AKAP	Low accuracy

IV. EXPECTED CONCLUSION

The fundamental complaints of my theory work are as per the going with:

1. To lessen execution time from cloud specialist co-ops.
2. To lessen execution time from cloud client.
3. To lessen correspondence cost.

REFERENCES

[1] Poorvika Singh Negi, Aditya Garg and Roshan Lal, "Intrusion Detection and Prevention using Honeypot Network for Cloud Security", IEEE Conference on data security, 2020.

[2] Yang Ming and Hongliang Cheng, “Efficient Certificateless Conditional Privacy-Preserving Authentication Scheme in VANETs”, Hindawi Mobile Information Systems, 2019.

[3] Feifei Wang , Guoai Xu and Lize Gu. “A Secure and Efficient ECC-Based Anonymous Authentication Protocol”, Security and Communication Networks Volume 2019.

[4] Yicheng Yu, Liang Hu and Jianfeng Chu, “A Secure Authentication and Key Agreement Scheme for IoT-Based Cloud Computing Environment”, www.mdpi.com/journal/symmetry, 2019.

[5] Xiaoying Jia, Debiao He , Neeraj Kumar and Kim-Kwang Raymond Choo, “A Provably Secure and Efficient Identity-Based Anonymous Authentication Scheme for Mobile Edge Computing”, IEEE SYSTEMS JOURNAL, 2019.

[6] Hamza Hammami, Sadok Ben Yahia, Mohammad S. Obaidat, "A lightweight anonymous authentication scheme for secure cloud computing services", The Journal of Supercomputing, 2019.

[7] Adesh Kumari, Vinod Kumar, M. Yahya Abbasi, Mansaf Alam, "The Cryptanalysis of a Secure Authentication Scheme Based on Elliptic Curve Cryptography for IOT and Cloud Servers", International Conference on Advances in Computing, Communication Control and Networking (ICACCCN2018), 2018.

[8] Linmei Jiang, Xiaochao Li, L.L. Cheng and Donghui Guo, "Identity Authentication Scheme of Cloud Storage for User Anonymity via USB Token", IEEE International Conference on Cloud Computing, 2018.

[9] Qi Xie, Duncan S. Wong, Guilin Wang, Xiao Tan, Kefei Chen, Liming Fang, "Provably Secure Dynamic ID-based Anonymous Two-factor Authenticated Key Exchange Protocol with Extended Security Model", IEEE Transactions on Information Forensics and Security, 2017.

[10] Yaser Mansouri, Adel Nadjaran Toosi and Rajkumar Buyya, "Cost Optimization for Dynamic Replication and Migration of Data in Cloud Data Centers", IEEE Transactions on Cloud Computing, 2017.

[11] F. Abundiz-Pérez, C. Cruz-Hernández, M. A. Murillo-Escobar, R. M. López-Gutiérrez and A. Arellano-Delgado, "A Fingerprint Image Encryption Scheme Based on Hyperchaotic Rössler Map", Hindawi Publishing Corporation Mathematical Problems in Engineering Volume 2016.

[12] Kuo-Hui YEH, "A lightweight authentication scheme with user un-traceability", Frontiers of Information Technology & Electronic Engineering, 2015.

[13] Preeti Chandrakar, Hari Om , "A Secure Two-Factor Mutual Authentication and Session Key Agreement Protocol using Elliptic Curve Cryptography", IEEE International Conference on Computer Graphics, Vision and Information Security (CGVIS), 2015.

[14] Shehzad Ashraf Chaudhry, Husnain Naqvi, Taeshik Shon, Muhammad Sher, Mohammad Sabzinejad Farash, "Cryptanalysis and Improvement of an Improved Two Factor Authentication Protocol for Telecare Medical Information Systems", Springer Journal (10.1007/s10916-015-0244-0), 2015.

[15] Yanrong Lu, Lixiang Li, Haipeng Peng, Yixian Yang, "An anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptography", Springer Journal of Multimedia Tools Application, 2015.

[16] Debiao He, Sherali Zeadally, Neeraj Kumar and Wei Wu, "Efficient and Anonymous Mobile User Authentication Protocol Using Self-certified Public Key Cryptography for Multi-server Architectures", IEEE Transactions on Information Forensics and Security, 2014.

[17] Mohammad Sabzinejad Farash, Mahmoud Ahmadian Attari, "A secure and efficient identity-based authenticated key exchange protocol for mobile client–server networks", Springer Journal of Super Computing, 2014.

[18] Navneet Kambow, Lavleen Kaur Passi, "Honeypots: The Need of Network Security", International Journal of Computer Science and Information Technologies, Vol. 5 (5), 2014.

[19] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, "An analysis of security issues for cloud computing", Journal of Internet Services and Applications, 2013.

[20] Ren-Chiun Wang, Wen-Shenq Juang, Chin-Laung Lei, "Robust authentication and key agreement scheme preserving the privacy of secret key", Elsevier journal of computer communication, 2011.