INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 11 Issue: 02 | April - June 2020
Paper is available at http://www.jrps.in | Email : info@jrps.in

A REVIEW ON SECURITY ISSUES IN CLOUD ENVIRONMENT

Anurag sharma, anuragsharma337@gmail.com
Miss pooja (Assistant professor), dulguchpooja454@gmail.com

Abstract:. It has been observed that Cloud computing provides twenty four hour Support and it allows Easy & Agile Deployments. As its need is growing day to day, there is need to improve the security of cloud. This paper has discussed the cloud computing requirement and threats to its security. Moreover the various types of attack over cloud network and security mechanisms are considered. The existing research along with their methodology has been discussed in this paper. Finally the need and scope of security in cloud environment has been explained here. Moreover in order to enhance the performance of data transmission in cloud network its would be better to compress data after encryption.

ISSN : 2278-6848 03
9 772278 684800
© International Journal for Research Publication and Seminar

Index terms: CLOUD, SECURITY, ENCRYPTION, RSA, ATTACK, WSN.

I. INTRODUCTION

Cloud computing is considered as a mechanism to deliver information technology services. Here resources have been retrieved from Internet using web-based tools. It is opposed to a direct connection to a server. Rather than keeping files on a proprietary hard drive or local storage device, cloud-based storage makes it possible to save them to a remote database. As long as an electronic device has access to the web, it has access to the data and the software programs to run it. It's called cloud computing because the information being accessed is found in "the cloud" and does not require a user to be in a specific place to gain access to it. This type of system allows employees to work remotely. Companies providing cloud services enable users to store files and applications on remote servers, and then access the data via the internet.

FIGURE 1 CLOUD COMPUTING

Cloud might be internet or network. It gives services over network which may be public or private. Cloud is available at remote location. They have been utilized in wide area network as well as in local area network. It may be used in virtual private network too. Lot of application such as email & web dependent conferencing usually implemented over cloud. Cloud computing has offered Platform independency as there is no necessity in order to set specific software on computer.

Thus it could be said that present business applications are mobile. They are collaborative because of cloud computing. There are many services that are making cloud computing more feasible. They are also making it easy to access for operator.

Proponents claim is that give authority to enterprises to fetch applications up with fast execution. It enables IT teams to fast set resources to fulfill changeable non predictable claim related to business. It is done with better manageability low amount of maintenance. It may be lead to high cost if administrator in not going accept cloud price model unexpectedly. It is considered as providers that are typically utilized salaries when someone went model. Inexpensive computers system as well as storage space devices such as widespread acceptance of hardware virtualization, autonomic & utility computing, service oriented structural design led to a development in it during availability of highly powered networks. Enterprises may scale up because computing requires raise and then low scale when demands get decreased.

Requirement of Cloud Computing

1. Cloud computing provides twenty four hour Support
2. Cloud computing allows Easy & Agile Deployments.
3. Cloud computing pay as we use
4. Cloud computing is providing scalability, Reliability, sustainability.
5. Cloud computing is having less Total Cost of possession
6. Cloud computing has been providing Secure Storage Management Expenditure.
7. Such systems are Highly Automated.
8. Cloud computing is competent to Free up (IR)Internal Resources.
9. Such Systems are Utility Based.
10. Cloud computing are Device & area Independent.

II. INTRODUCTION TO DATA SECURITY

Security is an essential aspect of IT for organizations of every size and type. Security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers databases websites. Data security also protects data from corruption. So it has been considered big issues. These security technologies involve data masking, data removal backups.

A key data security technology measure is encryption, where digital data, software, hardware hard drives are encrypted therefore rendered unreadable to unauthorized users hackers [1]. At time of authentication, users must provide a password, code, biometric data, or some other form of data in order to verify his identity.

Types of data security are discussed here:

(i)Network layer security

TCP/IP could be made protected along within cryptographic techniques internet protocols that have been designed for protecting emails on internet. These techniques of protocols consist of SSL TLS for traffic of website PGP for email Security of network contains IPSec.

(ii) IPSec Protocol

This method is developed for protecting interaction in a protected way using TCP/IP. It is a setup of security additions designed by IETF it gives security verification on internet protocol part by using method of cryptography. Information is modified using security methods. Major aspects of alteration that form reasons for internet protocol Section:-

(i) Authentication Header (ii) Encapsulating Security Payload

These two methods offer information reliability, information source verification anti service of reply. These methods of protocols are a mixture to offer chosen set of security solutions for layer of IP [2].

SECURITY OF NETWORK

Security of network is known as any activity that was made in order to secure usability integrity of computer network Information. It is consisting hardware as well as software technologies. It is focusing on variety of threats in order to prevent them from accessing computer network. The Effective Security of network is going to manage the access of network. Security of network is combining more than on layers of defense in network. Every Security of network layer is performing policies controls. The authorized users would be able to gain access to network resources but malicious actors may be blocked from performing threats related to exploits. Each company which needs to provide services that user's employees requirement should protect the network. Security of network also helps user to save proprietary data from hackers attack. It saves customers reputation [6]. Security of network is security given to a network from unauthorized access. This is the responsibility of network administrators to take preventive measures to save their networks from potential security threats.

III. RESEARCH GAP

This section includes literature survey to get basic information find scope of investigation, to develop Network threats for optimization of its different threats such as application layer attacks DOC, Passive, eavesdropping etc . Here in this section focus is on existing dissertation work related networks threats, issues related to data security in such networks security system used till now.

[14] Shari Mohammadi etal (2011): This paper focus on security of WSNs, divide it into four categories & will consider them, include: an overview of WSNs, security in WSNs, threat model on WSNs, a wide variety of WSNs' link layer attacks & a comparison of them. This work enables us to identify purpose & capabilities of attackers; furthermore, goal & effects of link layer attacks on WSNs are introduced. Also, this paper discusses known approaches of security detection & defensive mechanisms against link layer attacks; this would enable IT security managers to manage link layer attacks of WSNs more effectively.

[15] Wajeb Gharibi etal (2012): They think that advancement of new technology in general & social websites in particular will bring new security risks that may present opportunities for malicious actors, key loggers, Trojan horses, phishing, spies, viruses & attackers. Information security professionals, government officials & other intelligence agencies must develop new tools that prevent & adapt to future potential risks & threats. It can also safely manipulate huge amount of information in internet & in social websites as well.

[16] Tongguang Ni etal (2013): Based on characteristics of DDOS attack, this paper proposes a novel approach to detect DDOS attacks. Work provides two contributions: (1) HRPI is introduced to detect DDOS attacks, & it reflects essential features of attacks & (2) a detection scheme against DDOS attacks is proposed, & it can achieve high detection efficiency & flexibility. In our future work, we will make a detailed study of how to set all kinds of parameters in different application scenarios adaptively.

[17] Hong-Ning Dai etal (2013): They have explored using directional antennas in wireless sensor networks to improve Security of network in terms of reducing eavesdropping probability. In particular, we analyzed eavesdropping probability of single-hop networks & that of multi hop networks. We have found that using directional antennas in either a single hop network or a multi hop network could significantly reduce eavesdropping

probability. Security improvements of using directional antennas owe to smaller exposure region & fewer hops due to longer transmission range.

[18] Rupam etal (2013): This paper proposes an approach to detect packets through packet sniffing. It includes some negative aspects but besides these negative aspects it is much useful in snIffing of packets. Packet sniffer is not only used for hacking purpose but also it is used for network traffic analysis, packet/traffic monitoring, troubleshooting & other useful purposes. Packet sniffer is designed for capturing packets & a packet can contain clear text passwords, user names or other sensitive material. Sniffing is possible on both non switched & switched networks.

[19] **Sharmin Rashid etal (2013):** This paper describes use of IP spoofing as a method of attacking a network in order to gain unauthorized access & some detection & prevention methods of IP spoofing. Goal of attack is to establish a connection that will allow attacker to gain root access to host, allowing creation of a backdoor entry path into target system. We think that our proposed methods will be very helpful to detect & stop IP spoofing & give a secured communication system.

[20] Mukesh Barapatre etal (2013): This paper explain data security into client-server communication will be decreased. Thus, true WLAN security is always going to be a game of balancing acceptable risk & countermeasure to mitigate those risks. Understanding business risk, taking action to deter most important & most frequent attacks & following industry good practices gives us better security solutions.

[21] Amandeep Kaur etal (2014): Due to dynamic infrastructure of MANETs & having no centralized administration makes such network more vulnerable to many attacks. In this paper, we discuss about security challenges & how different layers protocols become vulnerable to various attacks. These attacks can classified as an active or passive attacks. Different security technologies are introduced to prevent such network. In future study we will try to invent such security algorithm, which will be work along with routing protocols that helps to reduce impact of different attacks.

[22] **Md. Waliullah etal (2014):** Securing wireless network is an ongoing process. Realistically, still there is no single true security measure in place. When a new technology is first introduced, hackers study protocol, look for vulnerabilities & then cobble together some program & scripts to try to exploit those vulnerabilities. Overtime those tools become more focused, more automated & readily available & published on open source network. Hence, they can be easily downloaded & run by anyone.

[23] P. Kiruthika Devi etal (2014): In this paper, various algorithms are proposed. Spoofing attack detection & localization in wireless sensor network have been extensively studied. There is no unique method for identifying & removing spoofing attack in wireless sensor network. Each method has its own advantages & disadvantages. Number of issues such as detecting presence of spoofing attacks, determining number of attackers, localizing multiple adversaries & eliminating them are not solved effectively. Further, this paper will help researcher to invent novel method in order to identify spoofing attack as well as remove or disable same in wireless sensor network effectively with less cost.

[24] Barleen Shinh etal (2014): Ad-hoc networks have become a new standard of wireless communication in infrastructure less environment. MANET is a Mobile Ad-hoc Network in which nodes get connected with each other without an access point. Messages are exchanged & relayed between nodes. Routing algorithms are utilized for forwarding packets between indirect nodes i.e. not in direct range with aid of intermediate nodes. They are spontaneous in nature & absence of centralized system makes them susceptible to various attacks. Black hole attack is one such attack in which a malicious node advertises itself as best route to destination node & hinders normal services provided by network. We conclude that multiple black hole attack is one of devastating attack done on network. Due to this attack packet loss may occur & delay increases.

[25] Ms. Vidya Vijayan etal (2014): There are many methods & techniques can conduct password cracking, in on-line or offline environment. Tools that can guess passwords for differential goals, & certain prevention tactics are presented here. This paper also focused on finding & documenting commonly available attacks on passwords. After analyzing all cracking strategies this paper enforce users to select passwords easy to remember but hard to guess.

[26] Blessy Rajra et al (2015): This paper describe Security of network is an important field that is increasingly gaining attention as internet expands. Security threats & internet protocol were analyzed to determine necessary security technology. Security technology is mostly software based, but many common hardware devices are used. current development in Security of network is not very impressive. This paper summarizes attacks & their classifications in wireless sensor networks & also an attempt has been made to explore security mechanism widely used to handle those attacks. This survey will hopefully motivate future researchers to come up with smarter & more robust security mechanisms & make their network safer.

[27] Venkadesh etal (2015): This survey paper gives knowledge regarding password stealing activities & protection mechanism available on online network communication. Protection of passwords is a vital activity in an on-line system. It

avoids vulnerable activities & anonymity loss of individual user. In future we attempt to implement a new mechanism from this survey that improves security against all kinds of attack.

[28] Thin Das etal (2016): In this paper, we proposed methodology for detecting identity-based attacks like spoofing attacks & hence localizing multiple adversaries in wireless sensor networks with high accuracy & precision. In contrast to conventional authentication methods, our RSS based scheme does not require any additional overhead to wireless sensor nodes. Our technique is use concept of Exploiting spatial correlation of RSS gained from wireless sensor nodes for attack detection & using PAM for clustering analysis for localizing multiple adversaries.

[29] Amandeep Kaur etal (2016): In wireless multi-hop sensor networks, an intruder may launch some attacks due to packet dropping in order to disrupt communication. To tolerate or mitigate such attacks, some of schemes have been proposed. But very few could effectively & efficiently identify intruders. Packet Droppers & Modifiers are common attacks in wireless sensor networks. It is very difficult to identify such attacks & this attack interrupts communication in wireless multi hop sensor networks. Today wireless communication technique has become an essential tool in any application that requires communication between one or more sender(s) & multiple receivers.

IV. TRADITIONAL ENCRYPTION MECHANISM

RSA has been considered an algorithm applied by modern computers in order to encrypt along with decrypt the information. This algorithm is an asymmetric cryptographic algorithm. By the word Asymmetric, means to say that there exists two separate keys. It has been also described as public key cryptography. Its cause is that any person may be get one of the keys.

The RSA algorithm includes the four phase. These are key generation, key distribution, encryption and decryption. A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, and if the public key is large enough, only someone with knowledge of the prime numbers can decode the message feasibly. Breaking RSA encryption is known as the RSA problem.

V. PROBLEM FORMULATION

It has been found the use of cloud is increasing day by day in present scenario. But the security issues are the biggest hurdle in the implementation of cloud infrastructures. Data travelling on Clouds have been influenced by attacks such as brute force and timing attack. There is need of security on session layer as well as application layer. However there are several techniques that have been proposed in order to provide security to cloud system. But they have certain limitations.

1. Existing security mechanism slows down the performance of cloud.
2. Time taken to secure data is some time more than that of transmission time.
3. The security is not available at all network layers.
4. Additional security reduces the transmission speed of data as it is process before and after receiving.
5. The encryption of data cannot prevent the destruction of data.

VI. SCOPE OF RESEARCH

The presented work is about to improve security of cloud computing with big data. In proposed work the concept of encryption and compression technique has been used. It is capable to offer security according to demands. It also enlarges the overall life time of network. It is possible by decrement of power consumption done by node. For optimization of local node, the network has been divided in smaller zones. Here the virtual coordinator on zone also identified. The coordinator will have the dealing statistics of zone nodes. Virtual coordinator would be done efficient hop selection according to routing performance.

REFERENCES

1. Amandeep Kaur, Dr. Amardeep Singh (2014) A Review on Security Attacks in Mobile Ad-hoc Networks, International Journal of Science & Research, Volume 3 Issue 5, might 2014
2. Md. Waliullah, (2014) Wireless LAN Security Threats & Vulnerabilities, International Journal of Advanced Computer Science & Applications, Vol. 5, No. 1, 2014
3. Jhilam Biswas, Ashutosh (2014) An Insight in to Network Traffic Analysis using Packet Sniffer, International Journal of Computer Applications (0975 – 8887) Volume 94 – No 11, might 2014
4. Blessy Rajra, A J Deepa (2015) A Survey on Network Security Attacks & Prevention Mechanism, Journal of Current Computer Science & Technology, Volume 5, No. 2, February 2015
5. Karun Handa, Uma Singh, "Data Security in Cloud Computing using Encryption and Steganography", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 4, Issue. 5, May 2015, pg.786 – 791.
6. ManpreetKaur, Hardeep Singh (2015) A review of cloud computing security issues International Journal of Advances in Engineering and Technology, June, 2015.

7. Amol C. Adamuthe, Vikram D. Salunkhe, Seema H. Patil (2015) Cloud Computing – A market Perspective and Research Directions I.J. Information Technology and Computer Science, 2015
8. Raj Kumar(2015) Research on Cloud Computing Security Threats using Data Transmission International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 1, January 2015 ISSN: 2277 128X
9. BurhanUl Islam Khan, Rashidah F. Olanrewaju, AsifaMehraj Baba(2015) Secure-Split-Merge Data Distribution in Cloud Infrastructure, IEEE Conference on Open Systems (ICOS), August 24-26, 2015
10. Jianghong Wei, Wenfen Liu, Xuexian Hu(2015) Secure Data Sharing in Cloud Computing Using
11. AL-MuseelemWaleed, Li Chunlin, "User Privacy and Security in Cloud Computing", International Journal of Security and Its Applications Vol. 10, No. 2 (2016), pp.341-352.
12. Nidal Hassan Hussein, Ahmed Khalid, "A survey of Cloud Computing Security challenges and solutions", International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 1, January 2016.
13. Babitha. M. P, K.R. RemeshBabu, "Secure Cloud Storage Using AES Encryption", International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), ©2016 IEEE.
14. SakshiChhabra, Ashutosh Kumar Singh(2016) Dynamic Data Leakage Detection model based approach for Map Reduce Computational Security in Cloud,
15. G.M.Nasira, Thangamani(2016) Securing Cloud Database By Data Fusing Technique (DFT) Using Cloud Storage Controller (CSC), 2016 IEEE International Conference on Advances in Computer Applications (ICACA)
16. Aaron Zimba, Chen Hongsong, Wang Zhaoshun(2016) An Integrated State Transition-Boolean Logic Model for Security Analysis in Cloud Computing 2016 First IEEE International Conference on Computer Communication and Internet
17. Suraj R. Pardeshi, Prof. Vikul J. Pawar, Prof. Kailash D. Kharat,(2017) "Enhancing Information Security in Cloud Computing Environment Using Cryptographic Techniques"
18. A. Bhardwaj, V. K. Singh, Vanraj, and Y. Narayan, "Analyzing BigData with Hadoop cluster in HDInsight azure Cloud," 12th IEEE Int. Conf. Electron. Energy, Environ.
19. P. R. Merla and Y. Liang, "Data analysis using hadoop MapReduce environment," Proc. - 2017 IEEE Int. Conf. Big Data, Big Data 2017, vol. 2018–Janua, pp. 4783–4785, 2018.
20. S. Narayan, S. Bailey, and A. Daga, "Hadoop acceleration in an openflow-based cluster,"
21. P. C. Neves, B. Schmerl, J. Bernardino, and J. Cámara, "Big Data in Cloud Computing : features and issues."2016
22. Y. Wang, I. Chen, V. Tech, and D. Wang, "A Survey of Mobile Cloud Computing Applications : Perspectives and Challenges," pp. 1–29.2013
23. M. A. Vouk, "Cloud Computing – Issues , Research and Implementations," pp. 235–246, 2008.
24. F. Lombardi and R. Di Pietro, "Secure virtualization for cloud computing," J. Netw. Comput. Appl., vol. 34, no. 4, pp. 1113–1122, 2011.
25. S. Mathew, "Implementation of Cloud Computing in Education - A Revolution," Int. J. Comput. Theory Eng., vol. 4, no. 3, pp. 473–475, 2012.
26. A. B. Angadi, A. B. Angadi, and K. C. Gull, "Security Issues with Possible Solutions in Cloud Computing-A Survey," vol. 2, no. 2, 2013.
27. S. V. K. Kumar and S. Padmapriya, "A Survey on Cloud Computing Security Threats and Vulnerabilities," vol. 2, no. 1, pp. 622–625, 2014.
28. M. Ahmed and M. Ashraf Hossain, "Cloud Computing and Security Issues in the Cloud," Int. J. Netw. Secur. Its Appl., vol. 6, no. 1, pp. 25–36, 2014.
29. S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing — The business perspective ☆" Decis. Support Syst., vol. 51, no. 1, pp. 176–189, 2014.
30. J. Teixeira, "Developing a Cloud Computing Platform for Big Data : The OpenStack Nova case," pp. 67–69, 2014.
31. Y. Wang, "Transplantation of Data Mining Algorithms to Cloud Computing Platform when Dealing Big Data," 2014.
32. M. Kaur and H. Singh, "A Review of Cloud Computing Security Issues," Int. J. Educ. Manag. Eng., vol. 5, no. 5, p. 32, 2015.