© INNOVATIVE RESEARCH THOUGHTS | Refereed | Peer Reviewed | Indexed
ISSN : 2454 – 308X | Volume : 07 , Issue : 04 | October - December 2021

A REVIEW ON SECURITY ISSUES IN CLOUD ENVIRONMENT

Seema Sangwan
Assistant professor computer science
Pt N.R.S Govt college Rohtak.
Email id: cma.sangwan124001@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.

Key Words: CLOUD, SECURITY, ENCRYPTION, RSA, ATTACK, WSN.

I. INTRODUCTION

Computing in the cloud is an option for providing IT services. In this instance, web-based instruments have been used to obtain online materials. It's an alternative to linking straight to a server. Cloud-based storage allows users to save their data in a distant database rather than on a dedicated server or local storage device. As long as a computer or other electronic device can connect to the internet, it has access to all of the information and applications it needs to function properly. Computing in the cloud gets its name from the fact that users need not physically be near a server in order to access data stored there. The use of such a technology facilitates telecommuting. Users may access their data and programmes stored on faraway servers via the cloud service provider's website.

FIGURE 1 CLOUD COMPUTING

Cloud may refer to the web or a computer network. It provides access to its resources through a network, either public or private. You may access the cloud from afar. They have found use in LANs and WANs alike. Possible applications include VPNs. Email and web-based conferencing are only two examples of the many applications that are often deployed in the cloud. Thanks to cloud computing, there is no longer any need to install platform-specific software on individual computers.

It follows that modern business apps are, in a sense, mobile. On part, this is due to the fact that their work is now being done in the cloud. Numerous offerings facilitate cloud computing's widespread adoption. They are also making it simple for the operator to get access.

One of the main arguments in favour of this approach is that it gives businesses more leeway in terms of how quickly they can deploy new apps. It paves the way for IT departments to rapidly allocate resources to meet changing, unpredictable business demands. This is achieved with little effort and maximum benefit. Unexpectedly huge costs might result if administrators

refuse to adopt the cloud's pricing paradigm. When someone goes into the modelling business, they are seen as a provider and their salary is adjusted accordingly. The widespread use of hardware virtualization, autonomic & utility computing, service oriented structural design, and so on, in conjunction with the availability of highly powered networks, facilitated its development. Businesses may choose to scale up in response to increased computing needs and then scale back down when demand declines.

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

For businesses of all sizes and in a wide variety of industries, IT security is a must. Security procedures are those used to safeguard the confidentiality, integrity, and availability of digital resources, such as files, programmes, and websites. As an added bonus, data integrity is preserved when proper safeguards are in place. Therefore, it is a major concern. Data masking and data deletion backups are examples of these security measures.

Encryption is a critical data security technology measure because it makes digital data, software, and physical hard drives unreadable to unauthorised users and hackers [1]. In order to prove his identity, a user must provide a password, code, biometric data, or any other type of data at the moment of authentication.

Many different types of data security are covered:

(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

Network security refers to the measures used to protect the confidentiality, availability, and integrity of data sent through a network. It incorporates both hardware and software innovations. The goal is to block a wide range of potential dangers from entering the system. Network access will be controlled by the efficient network security system. There are several levels of protection in place to keep your network safe. Each and every layer of the network

enforces security regulations. However, bad actors may be prevented from launching exploit-related attacks and gaining access to network resources. A secure network is a need for every business that wants to meet the demands of its workers. The protection of sensitive information is another benefit of a secure network for users. Customers' good names are preserved [6]. Network security refers to the protection of a network against intrusion. In order to protect their networks from harm, it is the duty of network administrators to implement preventative measures.

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

Many current computers use RSA as a technique for both encrypting and decrypting data. It is an asymmetric cryptography algorithm. To remark that there are two distinct keys is what is meant by the term "asymmetric." Public-key cryptography is another name for it. The fact that anybody may theoretically get a key is a major contributing factor.

There are four stages to the RSA algorithm. There are four main steps: creating keys, sharing keys, encrypting data, and decrypting data. A user of RSA generates a public key consisting of two huge prime integers plus an auxiliary value and then makes it public. The primes should be kept hidden. The public key may be used to encrypt messages by anybody, but only someone who knows the prime numbers can decrypt them using the techniques now available in the literature, provided the public key is sufficiently big. The RSA issue is the challenge of breaking RSA encryption.

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.

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