Secure and Efficient Technique for Cloud Computing

Amandeep Kaur[1], Ramanjot Kaur[2]
[1]Research Scholar, [2]Assistant Professor
Doaba Group of college,PTU, Punjab, India

Abstract- The cloud computing is the architecture which is decentralized in nature. The security issues are the major issues of cloud computing. The various security attacks are broadly classified into active and passive attacks. The zombie attack is the active type of attack which affect network performance in terms various parameters. In the zombie attack, the malicious hosts spoof credentials and identifications of legitimate hosts. In this research work, technique of mutual authentication is designed which detect and isolate malicious hosts from the network. The proposed technique is implemented in MATLAB and performance is analyzed in terms of space utilization, time and bandwidth consumption.

Keywords- Attack, Zombie, Mutual Authentication

I. INTRODUCTION

Cloud computing is the environment which provides on-demand & convenient access of the network to a computing resources like storage, servers, applications, networks and the other services which can be released minimum efficiency way. User retrieved data and modified data which is stored by client or an organization in centralized data called cloud. Cloud is a design, where cloud service provider provides services to user on demand and it is also known as CSP stands for "Cloud Service Provider" [1]. It means that the user or the client who is using the service has to pay for whatever he/she is using or being used and served. It is a technique which gives a huge amount of applications under different-different topologies and each topology gives some new specialized services. The main goal of cloud computing is to realize the network is a high performance computer which is to allow users to put all services and information into cloud and get all kinds of services from cloud only through their Internet terminal equipment. What users see is a virtual view when they use cloud service, and the data and services are actually distributed at different locations in cloud [2]. The tendency that data and services will be converted to web is inevitable and more and more services and information will be in cloud. Cloud computing is a paradigm that focuses on sharing the information and computations over a scalable network of nodes. Examples are like nodes include end user computers, , and Web Services ,data centers and such a network of nodes as a cloud. An application based on these clouds is taken as a cloud application. cloud is a allegory for internet and is an abstraction for the complex infrastructure it conceals. The main idea is to use the existing infrastructure in order to bring all feasible services to the cloud and make it possible to access those services regardless of time and location. Network security, information security and many other security types like the computer security together make the term "Cloud Security". Because it consist all of the security mechanism given above. It gives the broad set of technologies, policies and controls that are used to secure the data and applications exist with the cloud computing environment [3]. It is not the product of computer security like anti-viruses and anti-spam's. Security is the most concerning point to any service. External security or internal security required to each field. Only security ensures the privacy and integrity the cloud data. There are many security loopholes exist in the service. The one of the model of deployment IaaS provides infrastructure collection in cloud computing like virtual machines, multiple computers and number of resources to users to store their application, information, confidential of file, document information etc. With the help of Amazon E2 service it is possible to map the internal cloud infrastructure and to identify where the exactly target virtual machine reside in the network [4]. After that instantiate new VMs until one is located co-resident with the target VM. After the successfully placement of instantiate VM to targeted VM then take out the confidential information from the targeted VM called as a Side channel attack. Side channel attack requires two main steps: Placement and Extraction. Placement refers to the challenger or attacker arranging to place their malicious VM on the same physical machine. Extraction: After successfully placement of the malicious VM to the targeted VM extract the confidential information, file and documents and other information on the targeted virtual machine. An attacker takes advantages of physically shared component in order to steal information from victim. Any co-resident user can launch co-channel attack. An attacker can effort to cooperation the cloud by insertion a malicious virtual machine in secure closeness to a final cloud server and then initiate a side channel attack [5]. Side-channel attacks have emerged as a type of successful security hazard targeting system completion of cryptographic algorithms. Evaluating a cryptographic system's resilience to side-channel attacks is therefore important for secure system design. Authentication is a pathetic point in hosted and virtual services and is frequently targeted. There are many different ways to authenticate users and these are based on what a person knows. The mechanisms used to protect the authentication process and the methods used are a common aim of attackers. Now the architecture of SaaS, IaaS, and Paas, is only IaaS offer this type of information security and data encryption. If the transmitted data is categorized to secret for any project then the cloud computing service is based on IaaS architecture. This will be the most correct result for safe data communication [6]. Moreover the authorization of data process or management for those data belonged to the enterprises but stored on the service provider's side must be approved by the user side.

II. LITERATURE REVIEW

Abdul Raouf Khan (2012) in his paper author discussed various features of attribute based access control scheme suitable for cloud computing environment [7]. It leads to the design of attribute based access control scheme for cloud computing. However, for a large distributed system like a cloud system access decision needs to be more flexible and scalable. This paper presents various access control technique used in cloud computing and highlights features of attribute based access control features which are important for designing an attribute based access control.

A. Akinbi (2013) they discussed security requirements for identity and access -+8in PaaS cloud infrastructure as a yardstick for measuring security frameworks and identification of security controls. they proposed an technique for identifying security controls needs in secured PaaS cloud environments by separating its individual components [8]. They identified threats to each component and possible industry standard security scheme which can be applied to mitigate such threats like distributed systems and virtualization. An IAM security framework was drafted from the holistic technique and security strategy to find security controls needs for a secured PaaS.

Abdulrahman Almutairi, et.al (2012), present a risk aware cloud virtual resources assignment for big datacenters and proposed two heuristics algorithms PBH partition based heuristic and SBH sharing based heuristic for scheduling to solve the assignment problem [9]. Develop efficient risk aware virtual resources assignment mechanism for cloud multitenant environment.

Ajey Singh, Dr. Maneesh Shrivastava (2012) in this paper they presented cloud computing is on the rise, and especially due to its enormous attraction to organized criminals, we can expect to see a lot of security incidents and new kinds of vulnerabilities around it within the decades to come [10]. This paper gives a first step towards classifying them, thus making them more concrete and improving their analysis. Being a work-in-progress, we will continue with the collection and classification of cloud-based attacks and vulnerabilities in order to prove or refute our attack taxonomy's applicability and appropriateness.

Bhavna Makhija, et.al (2013) described different existing paper techniques and their merits and demerits [11]. In all that papers some haven't described proper data security mechanisms some were lack in supporting dynamic data operations, some were lack in ensuring data integrity, while some were lacking by high resource and computation cost. Hence this paper gives overall clue of all existing techniques for cloud data security and methods proposed for ensuring data authentication using TPA (Third Party Auditor). There are two categories: private audit ability and public audit ability. Although private audit ability can achieve higher scheme efficiency, public audit ability allows anyone, not just the client (data owner), to challenge the cloud server for the correctness of data storage while keeping no private information.

Bibin K Onankunju (2013) author introduced a new technique for providing secured access control in cloud storage. This model gives a secure access control in cloud computing [12]. To provide more secured access control it adopts a hierarchical structure and it uses a clock. Using this we can easily delete, download and files from and to the cloud. It is a highly efficient model for provide access control in cloud computing. It is in a hierarchical structure and it using a clock for providing decryption key based on time.

III. RESEARCH METHODOLOGY

Access control is generally a policy or procedure that allows, denies or restricts access to a system. It may, as well, monitor and record all attempts made to access a system. Access Control may also identify users attempting to access a system unauthorized. It is a mechanism which is very much important for protection in computer security. Various access control models are in use, including the most common Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC). All these models are known as identity based access control models. In all these access control models, user (subjects) and resources (objects) are identified by unique names. Identification may be done directly or through roles assigned to the subjects. These access control methods are effective in unchangeable distributed system, where there are only a set of Users with a known set of services. The zzombie attack is possible in RB-MTAC which is possible and it will reduce the network reliability and security of the network will be compromised. To prevent the zombie attack, novel technique will be proposed which is based on the server identification. Before present its credentials to the server, legitimate client will ask sever for its credentials. If the sever credentials are verified by the client then further process will proceed otherwise algorithm will halt.

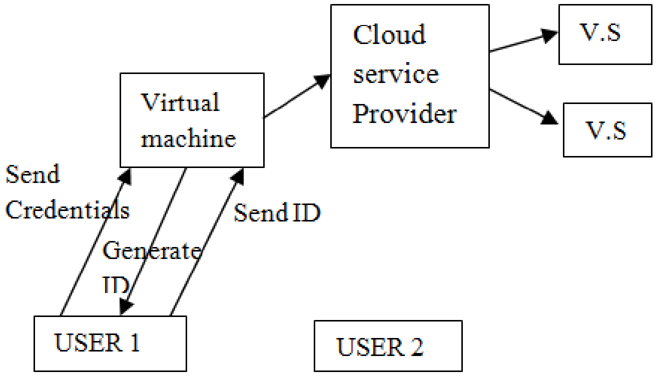

Fig.1: Flow diagram of proposed technique

As illustrated in figure 1, the proposed technique flow diagram. Following steps are implemented to isolate zombie attack:

1. **Send credential message**: This is the first step of proposed technique in which the user send its information of virtual machine. In the information user will send its MAC address, IP address and identification number
2. **Generate ID**: The virtual machine will receive the information from the user, if the information will match with the stored information on the virtual machine, then virtual machine will generate user identification. The generated ID will be encrypted with the public key of user. The user will decrypt the key with their private key
3. **Key presentation**: The user will send its generated key to the virtual machine, if the generated key will be verified by the virtual machine the access will be granted to user otherwise user will be detected as the malicious user.

IV. EXPERIMENTAL RESULTS

The proposed algorithm is implemented in MATLAB and results are analyzed in terms of execution time and space utilization.

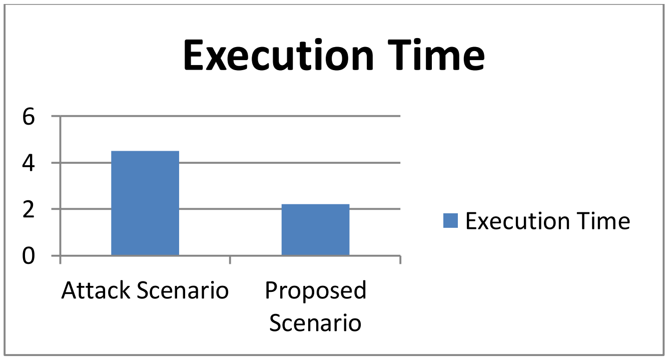

Fig.2: Execution Time Comparison

As shown in Figure 2, there is higher execution time of attack scenario as compared to the proposed scenario as the attack is isolated from the cloud scenario.

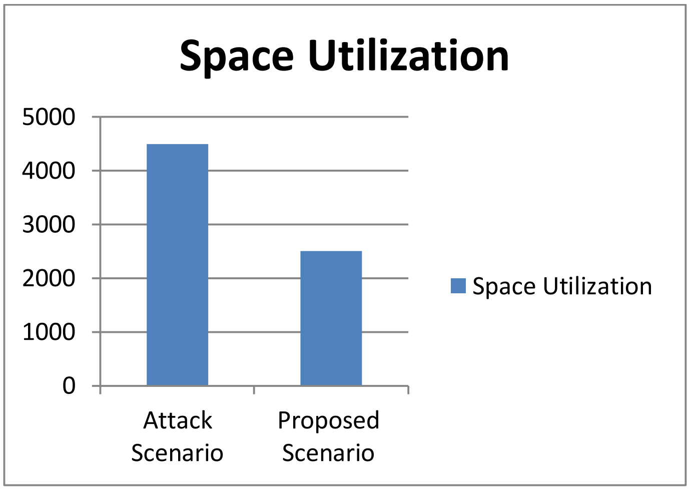

Fig.3: Space Utilization Comparison

As shown in Figure 3, there is reduction in buffer size when proposed scenario is applied in cloud systems as compared to previous attack scenario.

V. CONCLUSION

In this work, it is concluded that cloud architecture is decentralized in nature due to which various issues security issues raised in the network. The zombie attack is the active type of attack which reduces network performance in terms of certain parameters. In the zombie attack, malicious nodes spoof identification of legitimate nodes. The malicious nodes start communicating with the server on the behalf of legitimate nodes. In this research work, technique of mutual authentication will be proposed for the detection of malicious nodes. In the technique of mutual authentication, the nodes which are not able to prove its unique identification number is detected as malicious host. The proposed algorithm is implemented in MATLAB and results shows improvement in various parameters.

VI. REFERENCES

[1]. Reeja S L (2012) "Role Based Access Control Mechanism in Cloud Computing Using Co - Operative Secondary Authorization Recycling Method" International Journal of Emerging Technology and Advanced Engineering.

[2]. Shantanu Pal, Sunirmal Khatua (2011) "A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security"

[3]. Shucheng Yu (2010) "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing".

[4]. Young-Gi Min (2012) "Cloud Computing Security Issues and Access Control Solutions" Journal of Security Engineering.

[5]. Yu, Z., Wang, C., Thomborson, C., Wang, J., Lian, S., & Vasilakos, A. V. (2012). A novel watermarking method for software protection in the cloud.Software: Practice and Experience, 42(4), 409-430.

[6]. Sanjoli Singla, Jasmeet Singh (2013) “Cloud Data Security using Authentication and Encryption Technique” International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, July 2013

[7]. Khan, A. R. (2012). ACCESS CONTROL IN CLOUD COMPUTING ENVIRONMENT. Journal of Engineering & Applied Sciences, 7(5).

[8]. A Akinbi, E. Pereira, C. Beaumont (2013)“Identifying Security Methods and Controls for Secure PaaS Cloud Environments” International Journal of Emerging Technology and Advanced Engineering.

[9]. Abdulrahman A. Almutairi and Muhammad I. Sarfraz, Saleh Basalamah, “A Distributed Access Control Architecture for Cloud Computing”, 2012, IEEE SOFTWARE, PUBLISHED BY THE IEEE COMPUTER SOCIETY

[10]. Singh, A., & Shrivastava, M. (2012). Overview of Attacks on Cloud Computing. International Journal of Engineering and Innovative Technology (IJEIT), 1(4).

[11]. Bhavna Makhija, VinitKumar Gupta, (2013) “Enhanced Data Security in Cloud Computing with Third Party Auditor”, International Journal of Advanced Research in Computer Science and Software Engineering.

[12]. Bibin K Onankunju (2013) “Access Control in Cloud Computing” International Journal of Scientific and Research Publications, Volume 3, Issue 9.