Mutual Authentication Technique for Isolation of Virtual Side Channel Attack in Cloud Computing

Navneet Kaur, Supreet Kaur

Punjabi University Regional Centre for Information Technology and Management, Mohali, Punjab

Abstract - 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. Due to decentralized nature of cloud computing various security attacks are possible in the network. The virtual side channel attack is the active type of attack which degrade network performance in terms of various parameters. In this work, technique has been proposed which detect and isolate malicious nodes from the network. The proposed technique is implemented in MATLAB and performance is analyzed in terms of various parameters which shows that proposed technique is much efficient than the existing techniques

Keywords - Active Attack, Virtual Side Channel, 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 service. A public cloud is refers in which the infrastructure and services are provided off-site over the internet. These clouds offer the highest level of efficiency in shared resources but they are also more vulnerable than private clouds. Public clouds are executed by third parties and applications from different user are likely to be mixed together on the storage systems, networks and cloud servers [2]. A private cloud is referring in which the infrastructure and services are maintained on a private network. These clouds offer the highest level of security and control but there is a condition that they have require the organization or company to still purchase and maintain all the infrastructure and software which reduces the cost savings. A hybrid cloud environment in which consisting of multiple internal or external providers will be typical for many enterprises [3]. By integrating multiple cloud services users may be able to ease the transition to public cloud services while avoiding issues such as PCI compliance. Access control is concern with key because insider attacks are on top risk. A potential hacker is one who has been entrusted with approved access to the cloud. Anyone considering using the cloud requires looking at who is managing their information and which types of controls are applied to these individuals [4]. The traditional system of application centric access control in which each application keeps track of its collection of users and manages them which is not feasible in cloud based architectures. Because the user space maybe shared across applications that can lead to data storage replication and making mapping of users and their privileges a herculean task.

Virtual Side Channel Attack: 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 [5]. 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. 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 [6]. 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. Side-channel attacks have emerged as a type of successful security hazard targeting system completion of cryptographic algorithms.

II. LITERATURE REVIEW

Gouglidis Antonios (2011) This paper introduced and describe the definition of Cloud computing infrastructure containing associated concepts and characteristics. Access control models and authorization systems in the Cloud context are of vital importance due to their layered nature. Present access control models are not specifically designed to tackle the needs of Cloud model systems. By applying the conceptual classification for the Cloud model they describe how to find a list of basic access control's characteristics. In result they expect the applied methodology to initiate further research for the definition of access control needs in Cloud computing systems and moreover to result in new access control models [7].

Abdul Raouf Khan (2012) in his paper author discussed various features of attribute based access control scheme suitable for cloud computing environment. 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 [8].

Bhavna Makhija, et.al (2013) In this paper they described different existing paper techniques and their merits and demerits. 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). Third Party Auditor Third Party Auditor is kind of inspector. 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 [9].

Bhrugu Sevak (2012) Cloud computing is a word that delivering hosted service over the internet. This paper introduces how to avert the side channel attack in cloud computing. Using side-channel attack, it can be very easy to gain secret information from a device so it is good idea to provide security against side channel attack in cloud computing using combination of virtual firewall appliance and randomly encryption decryption (using concept of confusion diffusion) because it provides security against both front end and back end side of cloud computing architecture and also provide RAS (Reliability, Availability, and Security) [10].

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. 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 [11].

Chen Danwei (2011) discussed in this paper mainly cloud service security. Cloud service is based on Web Services and it will face all kinds of security issues including what Web Services face. The development of cloud service closely relates to its security therefore the research of cloud service security is a very important theme. This paper explain cloud computing and cloud service firstly and then gives cloud services access control model based on UCON and negotiation technologies and also designs the negotiation module [12].

III. RESEARCH METHODOLOGY

The proposed technique follows the steps that are to be implemented to isolate zombie attack:

1. **Send credential message**: This is the first step of proposed technique in which the user sends 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 matches will 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.

This process works between client and server.

For client:

1. Firstly Client has three values: gX , ID of client and MAC address.

2. Then these three values stored in H1 where H1 is parameter

$$H1= (gX+ ID+ MAC)$$

3. Then concatenate H1 with hash of id and mac address and x like H1|| (ID||MAC||x),

H2 = ID||MAC||x where x is shared secret between both client and server and H2 is second parameter

4. then client perform H1||H2|| (ID||MAC) and H3= (ID||MAC||nonce), where H3 is third parameter

5. Then client sends H1||H2||H3 to server

For server:

1. Server checks the H3 parameter values and match and nonce field of the client. The nonce field means request comes from the same the client which is requesting. The mac address also authenticate the client, if mac address and nonce field donot match than user is malicious

2. then again sever will check the H2 parameter values and again match the mac address with the mac address that is stored in its database, if again it's not match.

3. Then server match the shared secret value that is same between both client and the server, if these value is not matches, it means client is not genuine and server will detect it.

If the user is genuine, then server will perform:

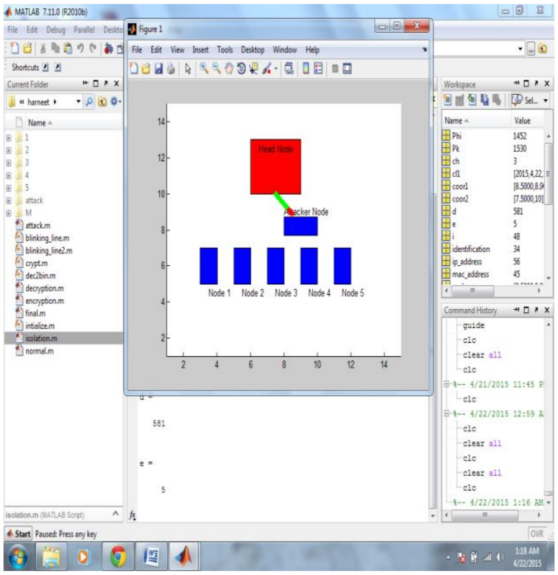
gX+ID+MAC / gID+MAC

and then computed value is gX.

If computed value is match with the genuine value of client, then it means client is legal.

IV. EXPERIMENTAL RESULTS

The proposed and existing techniques are implemented in MATLAB by considering various simulation parameters. It has been analyzed that execution time is reduced in proposed technique as compared to exiting technique



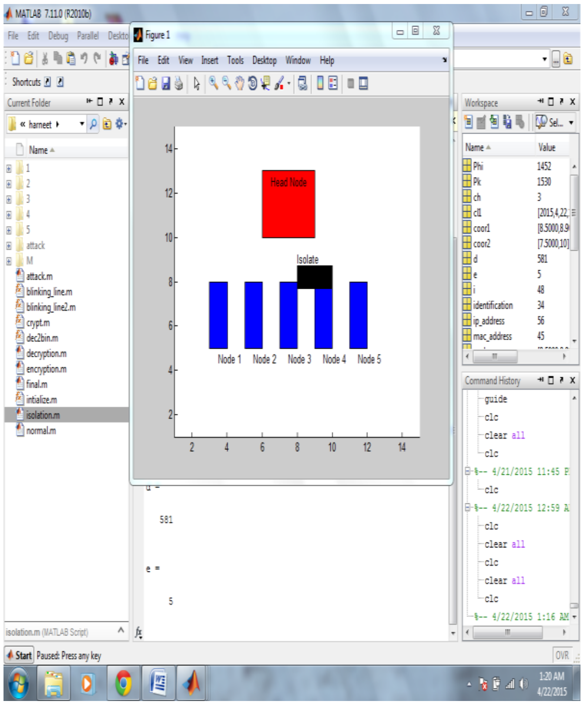
```
d =

581

e =

5
```

Name	Value
Phi	1452
Pk	1530
ch	3
cl1	[2015,4,22,
coor1	[8.5000,8.9
coor2	[7.5000,10]
d	581
e	5
i	48
identification	34
ip_address	56
mac_address	45

```
guide
clc
clear all
clc
%-- 4/21/2015 11:45 P
clc
%-- 4/22/2015 12:59 A
clc
clear all
clc
clear all
clc
%-- 4/22/2015 1:16 AM
```

Fig.1: Isolation of zombie attack

As shown in figure 1, the cloud network is deployed with the fixed number of user and cloud service provider. In this figure the user will enter the user with whose it wants to communicate. The attacker node enters the network to trigger zombie attack. When the cloud wants to communicate with the legitimate user each time it will forcefully communicate with the attacker node. The cloud node is asking for the identification number. The cloud node is asking for the MAC address of the user. The user is asking for the IP address of the user. The encrypted message is generated and it will be transferred to the user. The user will revert back the generated identification to the cloud for the verification.



```
d =

581

e =

5
```

Name	Value
Phi	1452
Pk	1530
ch	3
cl1	[2015,4,22,
coor1	[8.5000,8.9
coor2	[7.5000,10]
d	581
e	5
i	48
identification	34
ip_address	56
mac_address	45

```
guide
clc
clear all
clc
%-- 4/21/2015 11:45 P
clc
%-- 4/22/2015 12:59 A
clc
clear all
clc
clear all
clc
%-- 4/22/2015 1:16 AM
```

Fig.2: Isolation of zombie attack

As shown in figure 2, the cloud network is deployed with the fixed number of user and cloud service provider. In this figure the user will enter the user with whose it wants to communicate. The attacker node enters the network to trigger zombie attack. When the cloud wants to communicate with the legitimate user each time it will forcefully communicate with the attacker node. The cloud node is asking for the identification number. The cloud node is asking for the MAC address of the user. The user is asking for the IP address of the user. The encrypted message is generated and it will be transferred to the user. The user will revert back the generated identification to the cloud for the verification. The generated identification will not be matched and malicious node will be isolated from the network.

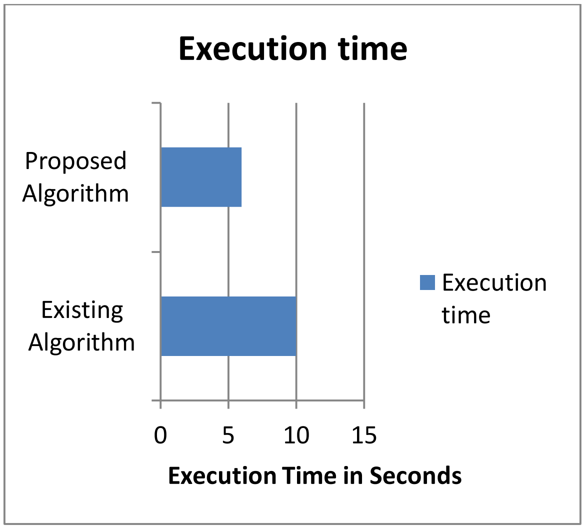


Fig.3: Execution Time Comparison

As shown in figure 3, The comparison of execution time of proposed and existing technique is shown and it has been analyzed that due to isolation of virtual side channel attack in the network, the execution time is reduced in proposed technique as compared to existing technique

V. CONCLUSION

The cloud computing is the architecture which is decentralized in nature and virtual machine, broker, cloud service provider, users are involved in the communication. Due to dynamic nature of the cloud computing various malicious nodes enter the network which is responsible to trigger various type of active and passive attacks. The virtual side channel attack is the active type of attack which degrades network performance in terms of various parameters. The mutual authentication based technique is proposed which detect and isolate malicious nodes from the network. In the proposed techniques each user provide its identification to the virtual machine and user which gets fail to prove its identification is detected as the malicious nodes. The performance of proposed and existing techniques are compared in terms of space utilization, energy consumption and it has been analyzed that proposed technique performs as compared to existing technique

VI. REFERENCES

[1]. Gitanjali (2013)" Policy Specification in Role based Access Control on Clouds" International Journal of Computer Applications (0975–8887) Volume 75– No.1.

[2]. Gerald Kaefer,(2010) "Cloud Computing Architecture", Corporate Research and Technologies, Munich, Germany, Siemens, Corporate Technology.

[3]. Ning, G., jiamao, L., xiaolu, C (2006) "Theory and Practice R & D of Web Services" p. 10. Machinery Industry Press.

[4]. Ramadan Abdunabi and Indrajit Ray (2008) "Extensions to the Role Based Access Control Model for Newer Computing Paradigms.

[5]. 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.

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

[7]. Gouglidis Antonios (2011)" Towards new access control models for Cloud computing systems" University of Macedonia, Department of Applied Informatics.

[8]. Khan, A. R. (2012). Access Control in Cloud Computing Environment. Journal of Engineering & Applied Sciences, 7(5).

[9]. 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.

[10]. Bhrugu Sevak (2012), "Security against Side Channel Attack in Cloud Computing" International Journal of Engineering and Advanced Technology (IJEAT), 2(2), December 2012

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

[12]. Chen Danwei, Huang Xiuli, and Ren Xunyi (2011) "Access Control of Cloud Service Based on UCON" Nanjing University of posts & Telecommunications.