Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 8, August 2017, pg.123 – 127

Technique for Detection of Malicious Nodes from Cloud Architecture

Sandeep Kaur, Usvir Kaur

Computer Science and Engineering Department, Sri Guru Granth Sahib World University Fatehgarh Sahib, India

Computer Science and Engineering Department, Sri Guru Granth Sahib World University Fatehgarh Sahib, India
Kaurnagah53@gmail.com; usvirkaur@gmail.com

Abstract*— The cloud computing is the architecture in which hosts, virtual machines and users are involved in the communication. The cloud is the decentralized nature due to which malicious nodes enter the network and trigger various types of attacks. The impersonate attack is the denial of service attack and it reduced the efficiency of the cloud architecture. In this work, zombie attack will be isolated and malicious virtual machines are detected from the cloud architecture. The proposed technique will be based on the mutual authentication mechanism. In this technique the unique number and OTP will assigned, before start of communication with the user. The machine will able to present it credentials to users. The massage exchanges are also developed in this work, between third party and virtual machine to detect malicious virtual machines.

***Keywords*— Cloud, RBAC, Attack, Zombie, MAC**

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 [1]. 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". 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. Access control is one of the most important security mechanisms in cloud service, and Cloud service can not apply the traditional access control model to achieve access control due to of its characteristics [2]. But there may be cloud services required to face the same security issues and Security needs and however one cannot separate from the traditional access control model ideas also. For Unauthorized Access issues they are often built on Delicate ID authentication and authorization. The mainly causes include: No authentication or fragile authentication To send the password and authentication information in plaintext. The system should adopt a strong authentication system and make encryption transmission to prevent unauthorized access [3]. 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 to look 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. It also needs the user to remember multiple passwords/accounts and maintain them.

Role Based Access Control (RBAC) has two phases to assign a privilege to a user. In first phase one or more roles are assigned to the users. In second phase, the roles are checked against the requested policies or operations. In RBAC (Role Based Access Control), permissions are not associated with user and it is associated with the roles [5]. Roles may have a hierarchical structure, reflecting the organization lines of responsibility and authority. In a RBAC model, all grant authorizations deal with roles. Users are then made members of roles and acquiring the roles authorizations. User access to resources is controlled by roles ach user is authorized to play certain roles and, based on his own role he can perform accesses to the resources and operate them correspondingly. As a role organizes a set of related authorizations together, it can simplify the authorization management [6]. Whenever a user needs a certain type of authority to perform an activity, user has to be granted the authority of a proper role, rather than directly assigned the specific authorizations. Furthermore, with Role-Based Access Control, decisions are based on the concept of user groups in access control. Roles are closely related to individual users have in an organization. Role based Access Control principles include: separation of duties, data abstraction and least privilege.

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 [7]. 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. 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:

a. Placement and Extraction: Placement refers to the challenger or attacker arranging to place their malicious VM on the same physical machine.

b. 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 [8]. An attacker takes advantages of physically shared component in order to steal information from victim. Any co-resident user can launch co-channel attack.

II. LITERATURE REVIEW

Mohamed Saied Emam Mohamed et.al (2011) present [9] improvements of the algebraic side-channel analysis of the Advanced Encryption Standard (AES) proposed. The experiments indicate that in both cases the amount of required side-channel information is less than the one required in the attacks introduced in. Furthermore, they introduce a method for error handling, which allows their improved algebraic side-channel attack to escape the assumption of an error-free measurement and thus become applicable in practice. They demonstrate the practical use of our improved algebraic side-channel attack by inserting predictions from a single-trace template attack.

Punithasurya K (2013) in this paper [10], a Novel Role Based Access Control technique is proposed to enhance the security requirement of cloud data storage which is named as secure cross domain access control. The proposed access control method include of the ABAC, DRBAC and RBAC. This technique minimizes the time constraints issue and Location constraints issues. Access control basically contains of access privileges based on the user needs. Provide security to the cloud is the major concern. Access control is required for most of the environment like grid, peer to peer and cloud. Most of the cloud computing infrastructure uses Role Based Access Control (RBAC).

Ramadan Abdunabi (2008) presented [11] the Role Based Access Control Model is the de facto standard consequently researchers have proposed numerous extensions to the classical RBAC model. Unfortunately they and in this work that there are quite a few new types of applications that implosive authorization requirements at the same time which are not stained by any of the proposed extensions of BAC. They outline a new authorization model to l this gap and conclude that there is still need of continued research in this are area. But notwithstanding its popularity RBAC has been found lacking in many computing applications.

Shucheng Yu (2010) this paper [12] describe challenging open issue by on one hand defining and enforcing access policies based on data attributes and on the other hand allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. They achieve this goal through exploiting and uniquely join techniques of attribute-based encryption (ABE), lazy re-encryption and proxy re-encryption. Their proposed method also has salient characteristics of user access privilege confidentiality and user secret key accountability. On observation shows that their proposed technique is highly efficient and provably secures under existing security system.

Shantanu Pa (2011) this paper [13], focuses on the development of a more secure cloud environment to find the trust of the service requesting authorities by using a novel VM (Virtual Machine) monitoring system. The proposed framework tries to maintain the domain reputation as long as possible by discarding

malicious users from the domain reducing the CSP's workload. It also increases some workload of domains and this framework fails to prevent malicious activity without CSP's information.

Shin-Jer Yang, et.al (2013), proposed a cloud service model [14], using identity management and Role-Based Access Control, under a multi –tenant architecture (MTA), to propose and design a Role-Based Multi-Tenancy Access Control (RB-MTAC). In RB-MTAC a user can be assigned many roles and each role is assigned too many permissions. This model combines identity management and role based access control method in multi tenancy cloud environment, to manage privileges for providing protect of the security of application and data privacy. For valid users, a role assignment capture roles corresponding to user from database and assign the role and access right which belong to the user.

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 zombie 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 the server for its credentials. If the sever credentials are verified by the client then further process will proceed otherwise algorithm will halt. Following steps are 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.

Experimental Results

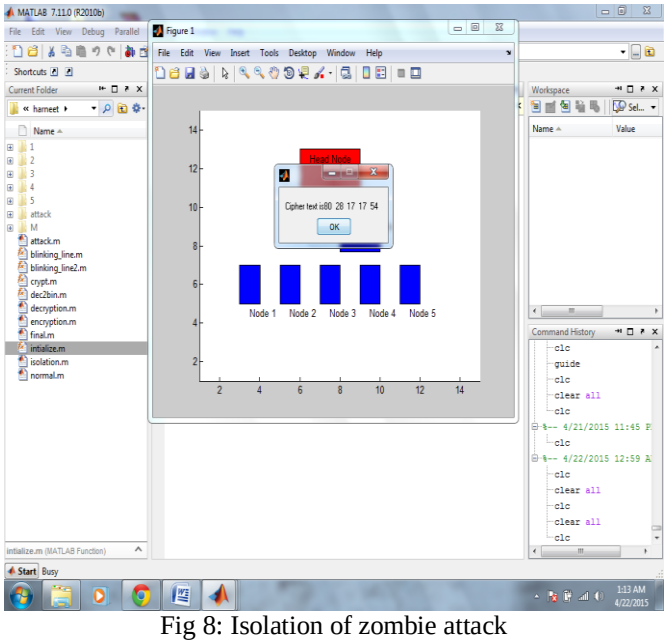

Fig 8: Isolation of zombie attack

As shown in figure 8, 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.

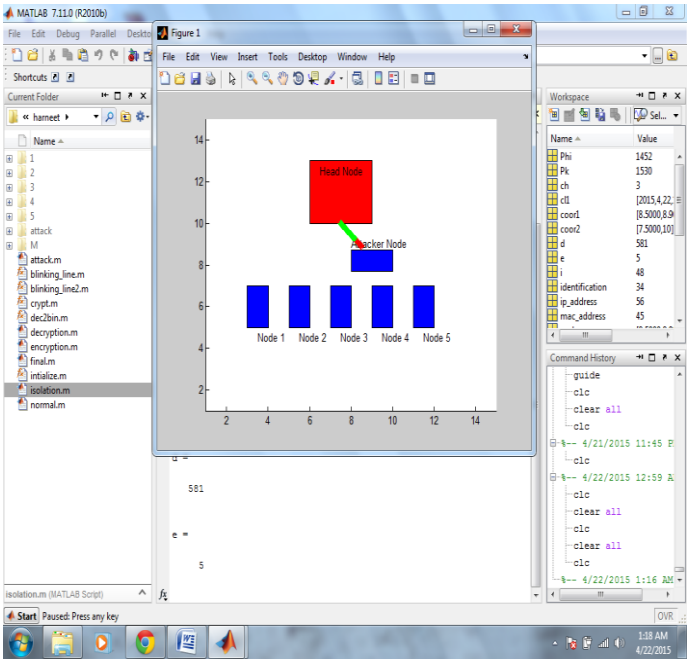

Fig 9: Isolation of zombie attack

As shown in figure 9, 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.

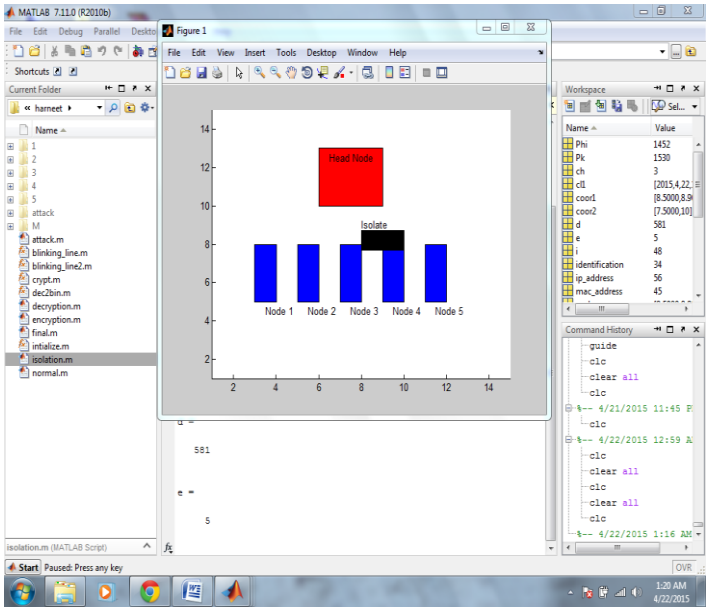

Fig 10: Isolation of zombie attack

As shown in figure 9, 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.

IV. CONCLUSIONS

In this work, it is been concluded that Cloud Computing is a set of IT Services that are provided to a customer over a network and these services are delivered by third party provider who owns the infrastructure and reduce the burden at user's end. Nowadays researchers devoted their work access control method to enhance the security on Cloud. RBAC is attractive access model because the number of roles is significantly less hence users can be easily classified according to their roles.

REFERENCES

[1] Foster, I., Zhao, Y "Cloud Computing and Grid Computing 360-Degree Compared", 2008, Grid Computing Environments Workshop
[2] Gouglidis Antonios, "Towards new access control models for Cloud computing systems", 2011, University of Macedonia, Department of Applied Informatics
[3] Gitanjali, "Policy Specification in Role based Access Control on Clouds", 2013, International Journal of Computer Applications (0975 – 8887) Volume 75– No.1
[4] Sanjoli Singla,Jasmeet Singh (july 2013) "Cloud Data Security using Authentication and Encryption Technique" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7
[5] Hamlen, K., Kantarcioglu, M., Khan, L., & Thuraisingham, B., "Security issues for cloud computing", 2010, International Journal of Information Security and Privacy (IJISP), 4(2), 36-48
[6] Bhrugu Sevak, "Security against Side Channel Attack in Cloud Computing" 2012, International Journal of Engineering and Advanced Technology (IJEAT), 2(2)
[7] Bhavna Makhija, VinitKumar Gupta, "Enhanced Data Security in Cloud Computing with Third Party Auditor", 2013, International Journal of Advanced Research in Computer Science and Software Engineering
[8] Barron, C., Yu, H., & Zhan, J., "Cloud Computing Security Case Studies and Research", 2013 International Conference of Parallel and Distributed Computing
[9] Mohamed Saied Emam Mohamed, Stanislav Bulygin, Michael Zohner, Annelie Heuser, Michael Walter, Johannes Buchmann, "Improved Algebraic Side-Channel Attack on AES", 2011, IACSA
[10] Punithasurya K, Esther Daniel, Dr. N. A. Vasanthi, 2013 "A Novel Role Based Cross Domain Access Control Scheme for Cloud Storage" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, March 2013, pp 942-946
[11] Ramadan Abdunabi and Indrajit Ray, "Extensions to the Role Based Access Control Model for Newer Computing Paradigms", 2008, IJARCSSE, volume 3
[12] Shucheng Yu "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", 2010, IEEE
[13] Shantanu Pal, Sunirmal Khatua, "A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security", 2011, IEEE
[14] Shin-jer,Yang pei-ci Lai, Jyhjong Lin, "Design role-based Multi-Tenancy Access control scheme for cloud services", international symposium on biometrics and security technologies, IEEE 2013

