To Propose a Novel Technique to Detect and Isolate Zombie Attack in Cloud Environment

Manish Kumar[1], Shivani Chauhan[2], Ajay Singh[3]
[1] Research Scholar, [2,3]Assistant professor,
Bhagwant Institute of Technology, Muzaffarnagar, UP, India.

Abstract - Cloud computing inevitable possess new challenges because traditional security mechanisms being followed are in sufficient to safeguard the cloud assests. Cloud Computing is easily can be targeted by the attackers. A group of malicious users or illegitimate users are attack on system and denial the services of legitimate users. Such kind of attacks are performed by the malicious (zombie) attackers. The zombie attack will degrades the network performance to large extend. In this paper RB-MAC technique has been proposed to isolate zombie attack.

Keywords - Cloud computing, Zombie, Access Control, RBMAC

I. INTRODUCTION

Cloud Computing is a biggest-scale distributed computing paradigm that is driven by economies of scale i.e. a pool of managed computing power, abstracted, dynamically-scalable, virtualized, storage, platforms and services are delivered on demand to external customers over the Internet [1]. Cloud is the network which is created through cloud service and computing model is the service provided in cloud. As we know Cloud Computing has become the hottest technology in IT world and is the research also focus in academic.

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 [2]. 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. 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 [3]. 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. The tendency that data and services will be converted to web is inevitable and more and more services and information will be in cloud.

A. Cloud Computing - 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 [4]. 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.

i). Service Models of Cloud Computing: The three service models are:

1) Cloud Software as a service (SaaS)
2) Cloud Platform as a Service (PaaS)
3) Infrastructure as a Service (IaaS**)**

SaaS : To use the provider’s applications running on a cloud infrastructure and accessible from various client devices through a thin client interface such as a Web browser.

PaaS : To deploy onto the cloud infrastructure consumer-created applications using programming languages and tools supported by the provider .

IaaS : To provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and application [4].

B. Attacks in Cloud Computing: There are many types of security issues as we discussed above are there in cloud computing. Due to these issues, attacks are possible in cloud. . There are various potential attack vector criminals may attempt such as:

i). Denial of Service (DoS) attacks - many security professionals have argued that the cloud is more vulnerable to DoS/DDOS attacks because this is shared by larger number of users which can makes DoS attacks much more dangerous .

ii). Side Channel attacks – An attacker could attempt to compromise the cloud through placing a malicious virtual machine in close proximity to a target the cloud server and then exploiting a side channel attack.

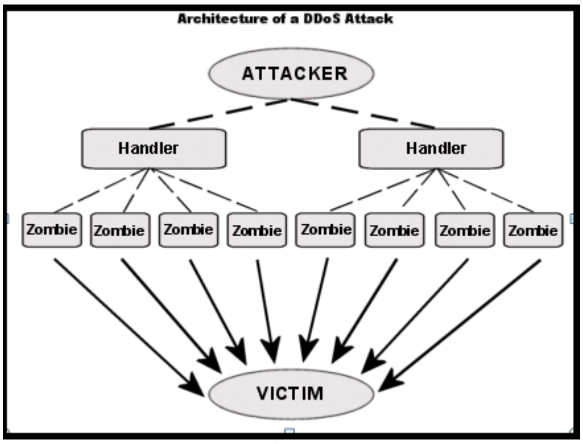

Figure 1: of DDOS attack

iii). Authentication attacks – Authentication is a weakest point in virtual services and hosted and is frequently targeted. There are many different kind of ways to authenticate users for example based on what a person knows, has, or is. The technology used to secure the authentication process and the scheme used are a frequent target of attackers.

iv). Man-in-the-middle cryptographic attacks – This type of attack is carried out when an attacker places himself between two communication parties. At anytime attackers can place themselves in the communication's path there is the possibility that they can intercept and modify communications message . An attack where a user between the receiver and sender of information and sniffs any data being sent. In some cases users may be sending unencrypted information which means the **man-in-the-middle** (**MITM**) can obtain any unencrypted data information. On other hand a user may be able to obtain information from the attack but have to unencrypted the information before it can be read.

II. REVIEW OF LITERATURE

In his paper [6] 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. **In paper [7]** they discussed security requirements for identity and access in 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. 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. In paper [8] presented 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. Develop efficient risk aware virtual resources assignment mechanism for cloud multitenant environment.

In this paper [9] 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. This paper gives a first step towards classifying them, thus making them more concrete and improving their analysis. Using the notion of attack surfaces, we illustrated the developed classification taxonomy by means of four up-to-date attack incidents of cloud computing scenarios. 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.

In this paper [10] proposed a cloud service model ,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 to many roles and each role is assigned to 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 .This model also block a non- tenant user accessing using identity management and access control prevent tenant users to viewing and accessing application and database without specific privilege .This method use a mechanism to manage user privilege using role based view point , and administrator only need to modify role privileges to change user privileges and thus reduce the potential errors from constant modifications.

III. ZOMBIE ATTACK

Zombie is one of the advance attack in cloud computing which degrade performance of the network and throughput of the network. In this there is a malicious node which act as a zombie of one of the connected user.

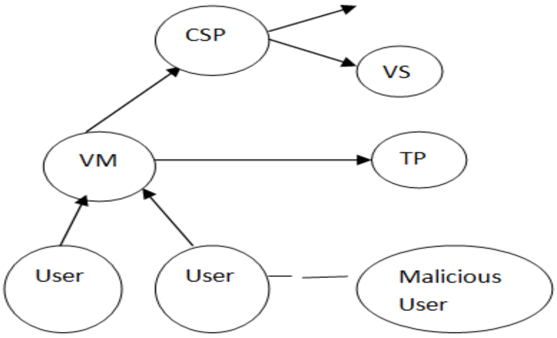

Figure 2: Zombie Attack

In fig.2 Virtual machine is there. VM is connected with Cloud service provider which is further connected with virtual server (VS). TP is a third party which is directly connected with virtual machine. There are number of users which are connected to virtual machines. There is also one malicious user which spoof credentials of connected user and act as a user. The whole process comes under zombie attack.

IV. PROPOSED METHODOLOGY

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. The Role-based Access Control (RBAC) model provides efficient way to manage access to information while reducing the cost of security administration and complexity in large networked applications. The Role based access control and identification based schemes are joined together and hybrid type of access control scheme is being developed. In the RB-MTAC applies identity management to determine the user's identity and applicable roles, since different users possess different functional roles with respective privileges for processing. Such role-based assignments can easily and efficiently manage a user's access rights to achieve application independence and data isolation for improving the processing performance of cloud multi-tenant services and hardening the security and privacy of cloud applications. The zombie attack is possible in RB-MTAC scheme. The enhancement will be done in RB-MTAC scheme to prevent the zombie attack. This will enhance security and reliability of cloud computing. 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 sever for its credentials. If the sever credentials are verified by the client then further process will proceed otherwise algorithm will halt. The proposed technique will be implemented in NS2.

V. EXPERIMENTAL RESULTS

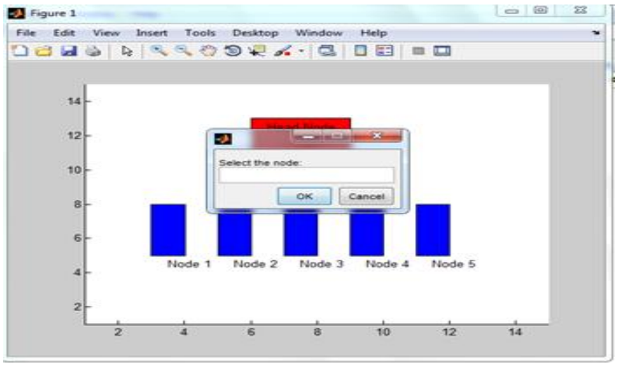

Figure 3: Network deployment

As shown in figure 3, 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.

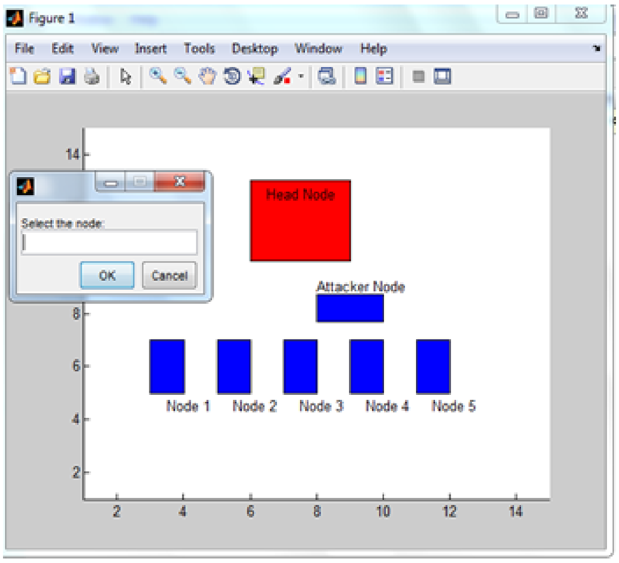

Figure 4: Trigger of zombie attack

As shown in figure 5.2, 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 want to communicate. The attacker node enters the network to trigger zombie attack.

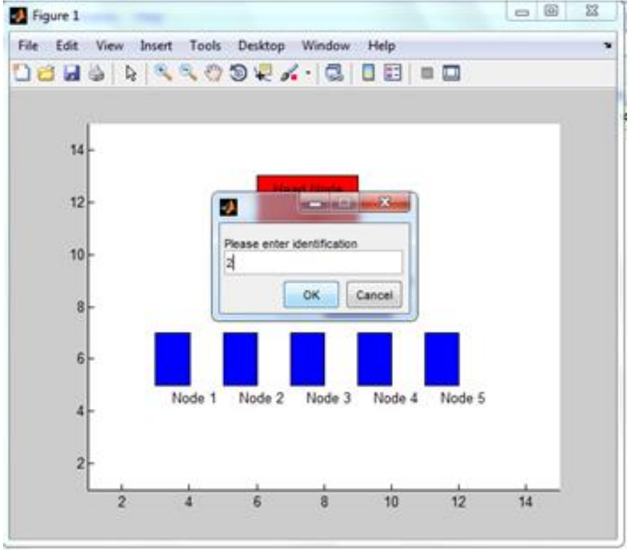
Figure 1
File Edit View Insert Tools Desktop Window Help
14
12
10
8
6
4
2
2 4 6 8 10 12 14
Please enter identification
2
OK
Cancel
Node 1
Node 2
Node 3
Node 4
Node 5

Figure 5: Isolation of Zombie Attack

As shown in figure 5, 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 want to communicate . The attacker node enters the network to trigger zombie attack. When the cloud wants to communicate with the legitimate user, every time it will forcefully communicates with the attacker node. The cloud node is asking for the identification number .

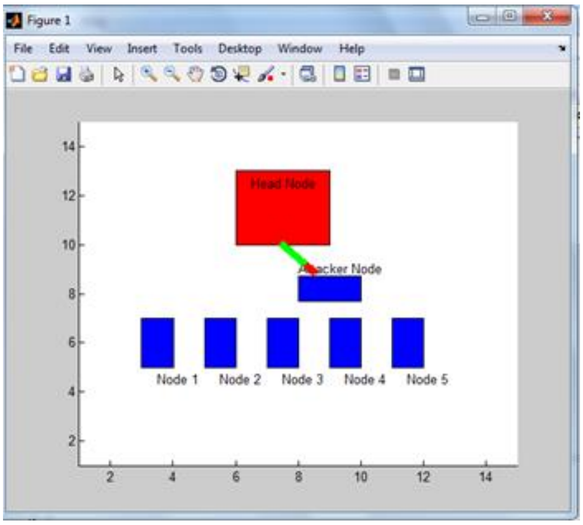

Figure 6: Isolation of zombie attack

As shown in figure 6, 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, every 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.

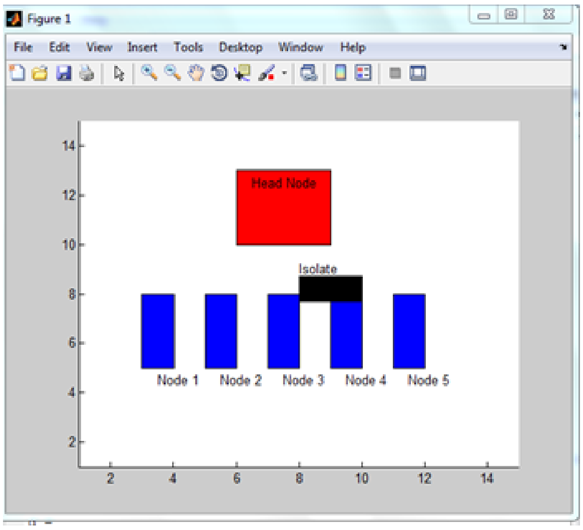

Figure 7: Isolation of zombie attack

As shown in figure 7, 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, every 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

VI. CONCLUSION

Cloud computing incorporates on-demand deployment, virtualization, open source software, and Internet delivery of services . The Cloud Computing Architecture which contains on-premise and cloud resources, middleware, , services, and software components, relocation, the externally visible properties of those and the relationships between them this is also refers as documentation of a system's cloud computing architecture. Due to this mobility increases and employees can access the information anywhere. There is capability of cloud computing to free-up IT workers who may have been occupied to performing factions like, installing ,updates and patches or involving inapplication support. As good services and benefit of Cloud Computing has to provided but there are security issues which make users unstable about the efficiency, safety and reliability in cloud computing. In proposed work we have implemented RB-MTAC scheme to prevent the zombie attack. This will enhance security and reliability of cloud computing. To prevent the zombie attack, novel technique has been proposed which is based on the server identification.

VII. REFERENCES

[1]. Foster, I., Zhao, Y(2008) "*Cloud Computing and Grid Computing 360-Degree Compared"* In: Grid Computing Environments Workshop.

[2]. 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.*

[3]. 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.

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

[5]. 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*

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

[7]. 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.

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

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

[10]. R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman,(1996) "*Role-Based access control models," IEEE Computer, 29(2):38-47.*

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

[12]. 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.*