ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY

An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**

www.computerscijournal.org

ISSN: 0974-6471
June 2017,
Vol. 10, No. (2):
Pgs. 338-344

Detection and Isolation of Zombie Attack under Cloud Environment

SUNIL KUMAR* and MANINDER SINGH

Department of Computer Science, Punjabi University, Patiala, India,.
*Corresponding author E-mail: sunilkapoorldh@gmail.com

http://dx.doi.org/10.13005/ojcst/10.02.12

(Received: March 21, 2017; Accepted: April 07, 2017)

ABSTRACT

Network security, data security and several other security types such as the computer security collectively compose the word “Cloud Security”. Cloud computing posses a new challenge because traditional security mechanism is being followed are insufficient to safeguard the cloud resources. Cloud computing can easily be targeted by the attackers. A group of malicious users or illegitimate users can attack on system which may lead to denial the services of legitimate users. Such kinds of attacks are performed by the malicious (zombie) attackers. The zombie attack will degrade the network performance to large extend. Traditional techniques are not easily capable to detect the zombie attacker in the cloud network. So in this paper we have proposed a technique which is the enhancement of the mutual authentication scheme in order to detect and isolate zombie attack for the efficient performance of the network.

Keywords: Cloud computing, Zombie, DoS, Attack.

INTRODUCTION

Cloud Computing is a largest-scale distributed computing paradigm that is driven by economies of scale i.e. a group of managed computing control, vague, dynamically-scalable, virtualized, storage, platforms and the services are delivered on demand to outside customers over the Internet. Cloud is the network which is formed through cloud service and computing model is the service provided in the cloud. As we know Cloud Computing has become the most recent technology in IT domain as well as the research also focus in intellectual. Cloud computing is the atmosphere which provides on-call & suitable access of the system to a computing resources like storage, networks , servers, applications, and the other services which can be out at minimum efficiency way. User retrieved data and customized data which is stored by customer or an association in centralized data called cloud. Cloud is a model, where cloud service provider administers services to user on-demand and it is also known as CSP which represents “Cloud Service Provider”. And it means that the customer who is using the service has to pay for anything that customer is using or being used or served. It is a technique which gives a vast amount of applications under different-different topologies and each topology provides several new specific services.

The major objective of cloud computing is to realize the network is a high performance computer which is to permit users to put all the services and information into cloud and get all kinds of services from cloud only through their Internet terminal tools. What users observe 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 to be expected and more and more services and information will be in cloud. As we know Cloud service is based on Web Services and Web Services are based on Internet. Internet has many its own inherent security weakness because of its openness and it has many other attacks and threats also. So that cloud services will face a big range of security problems. In present there are already many more security technologies for Web Services so this is great significance for us to resolve security issues of cloud service using this existing security information. Cloud computing is a model for facilitate suitable, on-demand network access to a common pool of configurable computing resources such as nets, grids, applications, servers, storage, and the services that can be quickly provisioned and get released with least management effort or service provider's communication. This cloud model improves availability and is composed of four deployment models, five significant characteristics along with three service models.

Service Models of Cloud Computing:

The three service models for cloud are:

- Cloud Software as a service (SaaS).
- Cloud Platform as a Service (PaaS) and
- Cloud Infrastructure as a Service (IaaS).

SaaS

To use the provider's applications running on a cloud infrastructure and available from different customer devices through a thin customer interface such as a Web browser.

PaaS

To set up on the cloud infrastructure customized applications using programming languages and tools supported by the provider (java, python, .Net)

IaaS

To provision processing, storage, networks, and other fundamental computing resources where the customer is able to establish and run any software, which can consist of operating system and applications.

The remainder of this paper is organized as follows: Section2 presents background information about Attacks in Cloud Computing. Section 3presents the Zombie attack working. Section 4 describe sour proposed method / Algorithm. Section 5 describes simulation environment and result discussions andsection6 concludes the paper.

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:

Denial of Service (DoS) attacks

many security specialized persons have contend that the cloud is more susceptible to DoS/DDOS attacks because this is shared by larger number of users which can create DoS attacks a lot more dangerous .

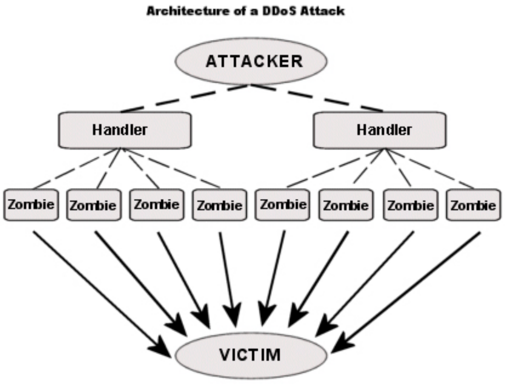


Fig. 1: DDOS Attack

Side Channel attacks

An attacker might try to compromise the cloud environment through placing a malicious virtual machine in close proximity to a target the cloud server and then take advantage of a side channel attack.

Authentication Attack

Authentication is a fragile point in virtual services as well as in hosted services 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 repeated aim of attackers.

Man-in-the-middle Cryptographic Attack

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 probability that they can capture and modify communications message. In some cases users may be sending unencrypted information which means that the man-in-the-middle (MITM) can obtain any unencrypted data information. On other hand a user may be able to get hold of information from the attack but have to unencrypted the information before it can be read.

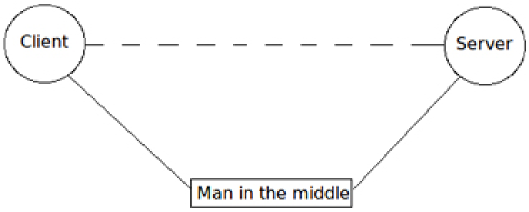


Fig. 2: Man in the Middle Attack

In the below figure is a sample of how a man-in-the-middle attack works. The attacker captures roughly or all traffics coming from the clients collect the information and then precede it to the target the user was initially intending to visit.

Inside-job

These kind of attack is when the staffs, person or employee or who is knowledgeable of how the system move from client to server after that he can embed malicious codes to harm everything in the cloud environment.

Zombie Attack in Cloud Environment

Zombie attack is one of the advance attacks in cloud computing environment which degrades degrade the performance of the network and throughput of the network. There are malicious nodes which act as a zombie of one of the connected users.

A system that has been inserted with a program that puts it under the control of malicious users without the awareness of the system user. Zombie is used by malicious users to launch DoS or DDoS attacks. Through an open communication

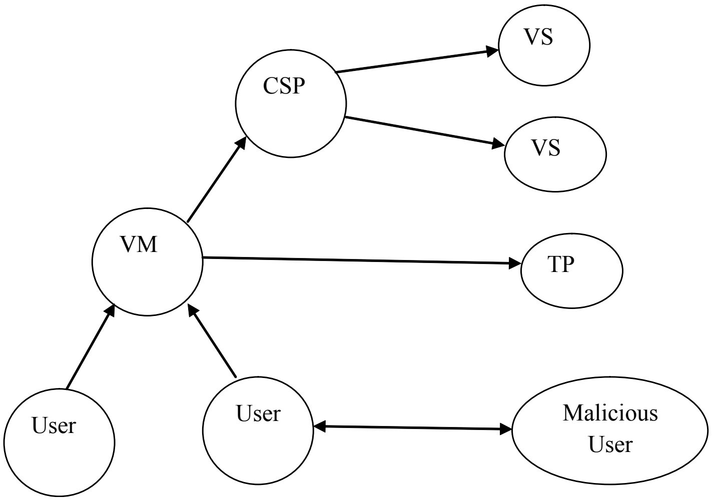


Fig. 3: Zombie Attack

port, the illegitimate user sends commands to the zombie. On command, the zombie system sends a huge amount of packets of worthless information to a targeted web site in order to block the site's router and keep genuine users from having access to the site. Traffic sent to web site is puzzling and as a result the system receiving the data use time and resource just to understand the flow of data has been sent out by the zombies.

According to above figure, Virtual Machine (VM) is described. VM is connected with cloud service provider (CSP) which is further connected with virtual server (VS). Third Party (TP) is available, 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 spoofs credentials of connected user and act as a user, the whole process comes under zombie attack.

METHODOLOGY

Access control is normally a procedure or process that permits, rejects or controls access to a system. It may also examine and record every attempt that is made to access a system. Access Control may, as well, identify users trying to access a system illegitimately. It is a mechanism which is especially significant for safety measures in computer security.

A variety of access control models are utilized, together with the most frequent (DAC) Discretionary Access Control, (RBAC) Role Based Access Control, and (MAC) Mandatory Access Control. All these models are recognized as identity based access control models. In these access control models, users (subjects) and resources (objects) are recognized by unique names. Identification may be made straightforwardly or through responsibilities given to the subjects. These access control techniques are efficient in constant distributed system, and there are only a set of users with a recognized set of services. The zombie attack is probable in RB-MTAC which is feasible and it will decrease the network dependability and the safety of the network will be compromised. To isolate the zombie attack, new technique will be proposed which is about the server credentials. Earlier, its identification to the server, rightful client will request the sever for its identification. If the sever identification are confirmed by the client then further process will carry on, if not algorithm will stop.

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

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.

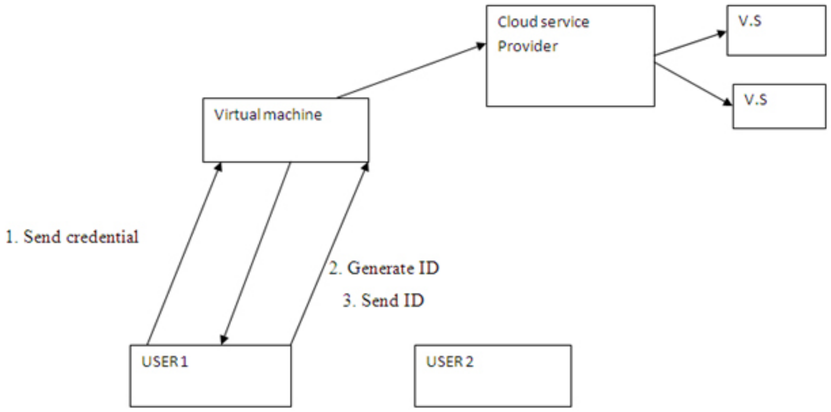


Fig. 4: Flow diagram of proposed technique

Generate ID

The virtual machine will receive the information from the user, if the information matches with the stored information on the virtual machine, then the virtual machine will create user identification. The generated ID will be encrypted with the public key of user. The user will decrypt the key with their private key

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.

Proposed Algorithm

In this process 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 client which is requesting. The mac address also authenticates the client, if mac address and nonce field do not 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 does not match.
3. Then server matches the shared secret value that is same between both client and the server, if this value doesn't match, 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 matches with the genuine value of client, then it means client is legal.

Simulation Environment & Result Discussion

We used the MATLAB 2013 for the practical environment. The proposed method, the cloud network is deployed with the fixed number of users and cloud service provider. There are five nodes and the client will enter the node to communicate with the cloud server but the attacker node will enter into the network to trigger zombie attack. In this attack, instead of client the attacker will communicate with the cloud server, detection and isolation of zombie attack with the proposed technique.

In fig 5, the user will enter the node data to communicate with the cloud server for the services of cloud. As shown in figure 6, the cloud network is deployed with the fixed number of users and cloud service provider. The attacker node enters the network to trigger zombie attack.

As shown in figure 7, the attacker node enters the network to trigger zombie attack and the cloud wants to communicate with the legitimate user, it will forcefully communicate with the attacker node every time. After this cloud node will ask about the identification number, the password for the authentication, shared key from the user, random key from the user, prime number from the user. After that the encrypted message is generated and it will be transferred to the user. The user will react back the created identification number to the cloud for the verification. In the final step, if the generated identification will not be matched and malicious node will be isolated from the network as shown in the figure 8.

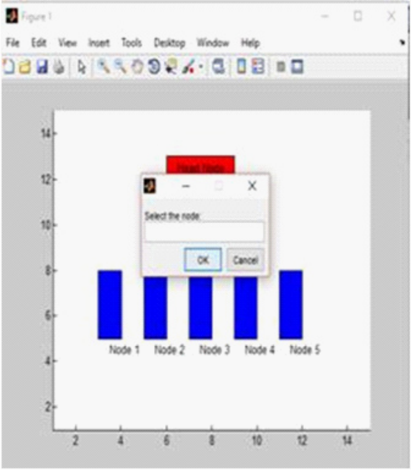


Figure 1
File Edit View Insert Tools Desktop Window Help
Head Node
Node 1 Node 2 Node 3 Node 4 Node 5
OK Cancel
2 4 6 8 10 12 14
2 4 6 8 10 12 14

Select the node:

Fig. 5: Network Deployment

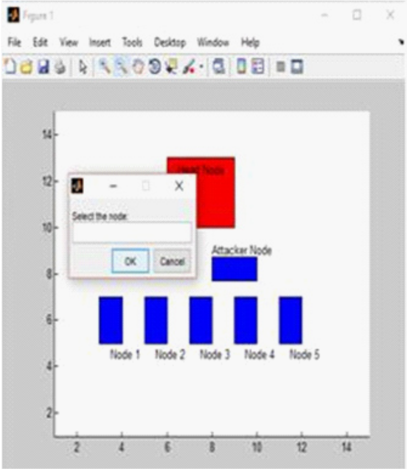


Figure 1
File Edit View Insert Tools Desktop Window Help
Head Node
Attacker Node
Node 1 Node 2 Node 3 Node 4 Node 5
OK Cancel
2 4 6 8 10 12 14
2 4 6 8 10 12 14

Select the node:

Fig. 6: Trigger of Zombie Attack

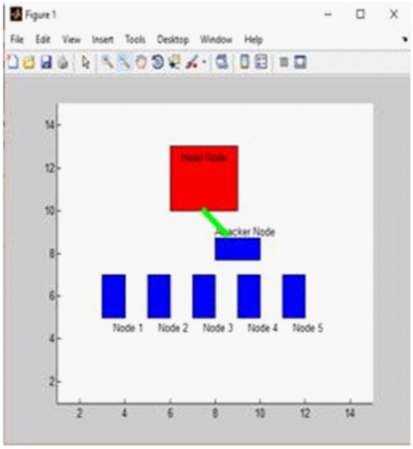


Figure 1
File Edit View Insert Tools Desktop Window Help
Head Node
Attacker Node
Node 1 Node 2 Node 3 Node 4 Node 5
2 4 6 8 10 12 14
2 4 6 8 10 12 14

Fig. 7: Trigger of Zombie Attack

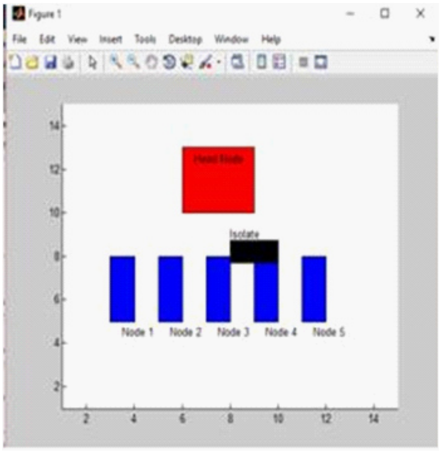
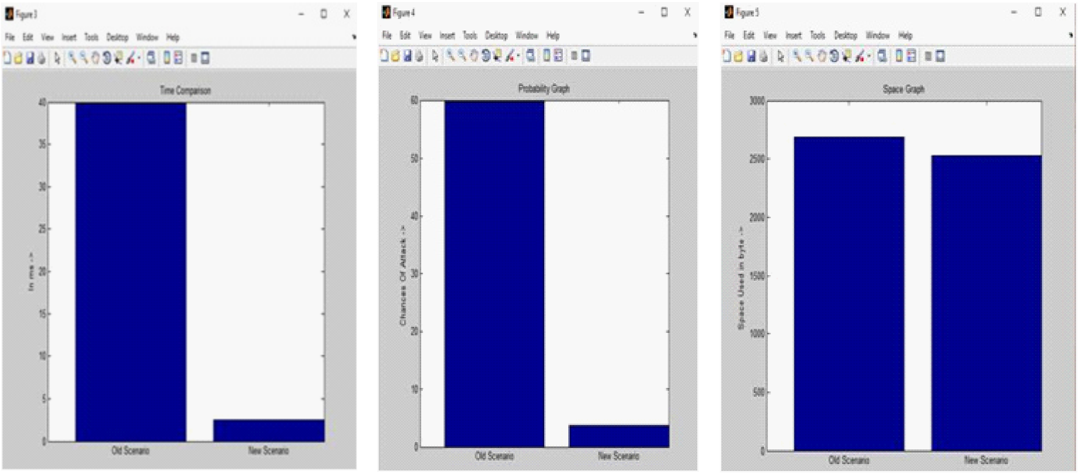


Figure 1
File Edit View Insert Tools Desktop Window Help
Head Node
Isolate
Node 1 Node 2 Node 3 Node 4 Node 5
2 4 6 8 10 12 14
2 4 6 8 10 12 14

Fig. 8: Isolation of zombie attack



(a) (b) (c)

Fig. 9: (a) shows the time comparison, (b) shows the probability comparison, (c) show the space comparison

CONCLUSION

As cloud computing faces various security issues which lead to the exposure of confidential data of users. These security issues make users unstable about the efficiency, safety and reliability in cloud computing. In proposed work, we have implemented mutual authentication scheme to prevent the zombie attack in cloud computing environment. A system that has been inserted with a program that puts it under the control of a malicious user without the awareness of the system user. Zombie is used by malicious user to launch DoS or DDoS attack. Through a open port, the illegitimate user sends the commands to the zombie. To detect and isolate the zombie attack we modify the mutual authentication scheme which produces the best results. This novel technique is based on the server identification.

REFERENCES

1. A.R.Khan, "Access Control in Cloud Computing Environment," *ARPN Journal of Engineering and Applied Sciences*, **7**(5), 2012.
2. Y. G. Min, Y.H.Bang, "Cloud Computing Security Issues and Access Control Solutions", *Journal of Security Engineering*, **2**, 2012.
3. M.Zhou, Y.Mu, W.Susilo, M.H.Au, "Privacy Preserved Access Control for Cloud Computing," IEEE International Joint Conference, 2011.
4. B. K. Onankunju,"Access Control in Cloud Computing"*International Journal of Scientific and Research Publications*, **3**(9), 2013.
5. M. George, C. Suresh, K. Saranya, "A Survey on Attribute Based Encryption Scheme in Cloud Computing" *International Journal of Advanced Research in Computer and Communication Engineering* **2**(11), 2013.
6. S. Chugh, S. Peddoju, "Access Control Based Data Security in Cloud Computing" *International Journal of Engineering Research and Applications* (IJERA) **2(**3**)**, 2012.
7. M. Ali, C. Pravallika, P. Srinivas, "Multi-Attribute Based Access Control Policy Enforcement for File Accesses in Cloud" *International Journal of Engineering Science and Innovative Technology* (IJESIT) **2(**5**)**, 2013.
8. D. Chen, "Data Security and Privacy Protection Issues in Cloud Computing" International Conference on Computer Science and Electronics Engineering, March 2012.
9. G. Ning, L.Jiamao, C. Xiaolu, "Theory and Practice R & D of Web Services" p. 10. Machinery Industry Press , 2006
10. D. Contractor, D.R.Patel, "Trust management framework for attenuation of application layer ddos attack in cloud computing", In: Trust Management VI, pp. 201–208. Springer, 2012.
11. T. Karnwal, S.Thandapanii, A. Gnanasekaran, "A filter tree approach to protect Cloud Computing against Xml DDoS and http DDoS Attack". In: Intelligent Informatics, pp. 459–469. Springer, 2013.
12. A.Shitoot, S. Sahu, R. Chawda, "Security Aspects in Cloud Computing", *International Journal of Engineering Trends and Technology* (IJETT)– **6**,2013.
13. S. Singla, J. Singh, "Cloud Data Security using Authentication and Encryption Technique" *International Journal of Advanced Research in Computer Engineering & Technology* (IJARCET) **2**(7), 2013.
14. B. Sevak, "Security against Side Channel Attack in Cloud Computing" *International Journal of Engineering and Advanced Technology* (IJEAT), **2**(2), 2012.
15. B. Makhija, V. Gupta, "Enhanced Data Security in Cloud Computing with Third Party Auditor", *International Journal of Advanced Research in Computer Science and Software Engineering*, 2013.
16. C. Barron, H. Yu, J. Zhan, "*Cloud Computing Security Case Studies and Research*". Proceedings of the World Congress on Engineering, **2**,2013.