www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 7 July 2017, Page No. 22079-22083
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i7.30

Technique for Isolation of Malicious Nodes from the Cloud Computing Architecture

Komal Jeet Kaur
komal.janjua@gmail.com

Abstract

The cloud computing is the architecture in which virtual machine, cloudlets, and data centers are involved in communication. In the network, malicious nodes are responsible to trigger various types of active and passive attacks which reduce network performance in terms of various parameters. In this work, technique will be proposed for the detection and isolation of malicious nodes from the network. the malicious nodes are responsible to trigger virtual side channel attack in the network.

Introduction

Cloud is the network which is created through cloud service and computing model is the service provided in cloud. 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]. 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. The tendency that data and services will be converted to web is inevitable and more and more services and information will be in cloud [2]. There are three cloud deployment model of cloud computing. 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 [3]. A private cloud is referring in which the infrastructure and services are maintained on a private network [4]. 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. There are many types of security issues in cloud computing. Due to these issues, attacks are possible in cloud [5]. 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. 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. [6] 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. 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 [7]. An attacker takes advantages of physically shared component in order to steal information from victim. Any co-resident user can launch co-channel attack.

Literature Review

Ajey Singh, Dr. Maneesh Shrivastava (2012) presented in this paper [8], that due to its enormous attraction of cloud computing to organized criminals, one 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. The process 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.

Bhrugu Sevak (2012) introduced in this paper [9], how to avert the side channel attack in cloud computing. This is accomplished by using combination of Virtual firewall appliance and random encryption decryption and provides RAS (Reliability, Availability, and Security) of client's data or information. 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 because it provides security against both front end and back end side of cloud computing architecture.

Chen Danwei (2011) discussed in this paper [10], 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.

Gouglidis Antonios (2011) discussed in this paper [11], 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. Based on the results metaphor from their analysis they believe that the design and implementation of proper access control models for the Cloud computing paradigm is required. 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.

Mohamed Saied Emam Mohamed et.al (2011) presented [12], improvements of the algebraic side-channel analysis of the Advanced Encryption Standard (AES) proposed. In particular, the paper optimizes the algebraic representation of AES and the algebraic representation of the obtained side-channel information in order to speed up the attack and increase the success rate. Their experiments indicate that in both cases the amount of required side-channel information is less than the one required in the attacks introduced in. The

authors demonstrate the practical use of our improved algebraic side-channel attack by inserting predictions from a single-trace template attack.

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 framework can be used to provide security in infrastructure, network as well as data storage in a heterogeneous cloud infrastructure. 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.

Research Methodology

The zombie attack is the active type of attack which is triggered by the malicious hosts in the network. The malicious host spoofs the credentials of the legitimate host that communicates with the cloud server on the behalf of legitimate user. This attack leads to reduction in network performance in terms of various parameters. In this work, technique will be proposed which will detect malicious hosts from the network. To detect malicious host technique of hash function is applied in the network. The legitimate host create the multiple has functions and value of final hash function is send to cloud server.

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 the client which is requesting. The mac address also authenticate 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'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.

DOI: 10.18535/ijecs/v6i7.30

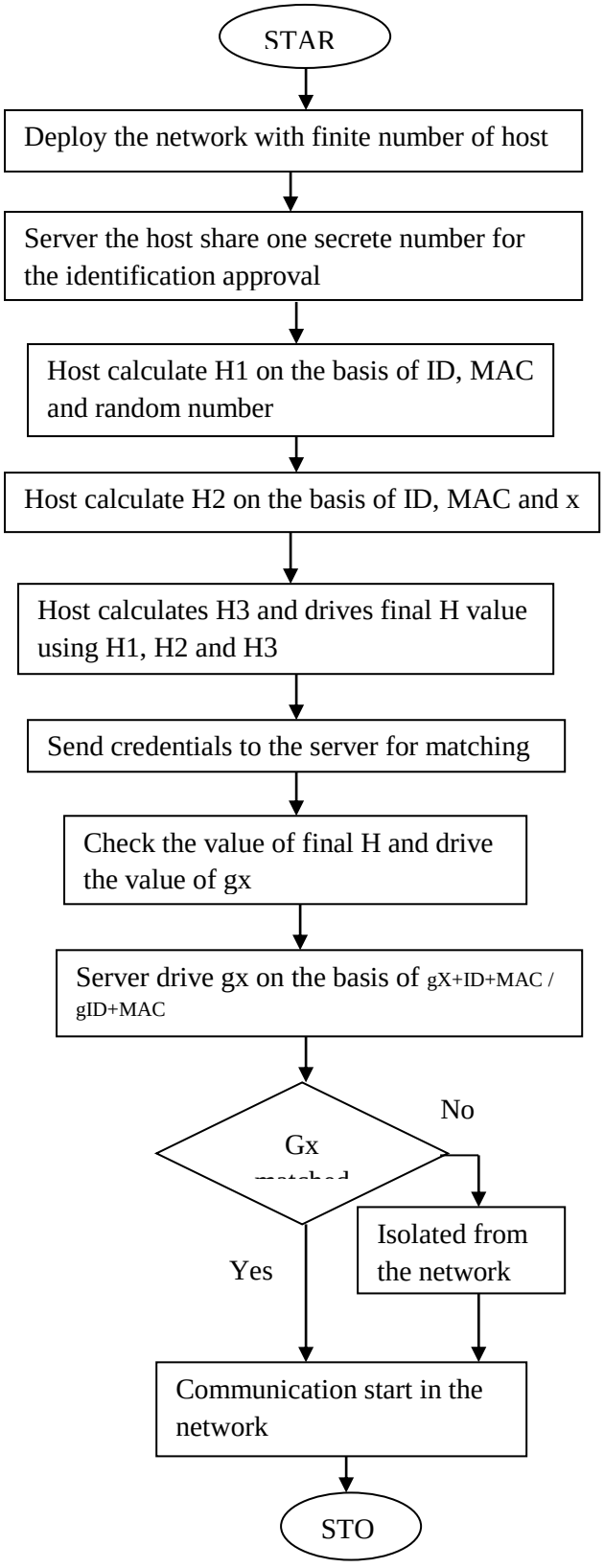

Fig 1: Proposed Flowchart

Experimental Results

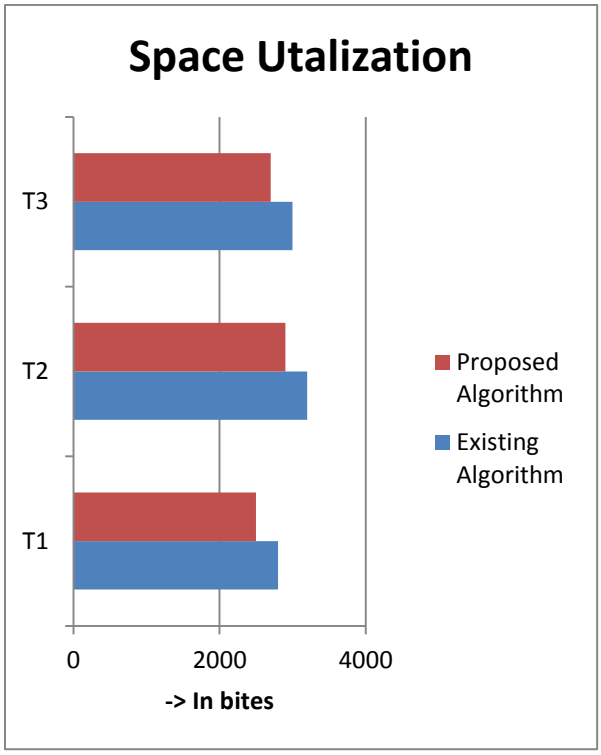

Fig 2: Space Utilization Comparison

As shown in the figure 2, the space of the existing and proposed technique is been compared and it is been analyzed that space in the proposed technique is less utilized due to improvement in the existing technique.

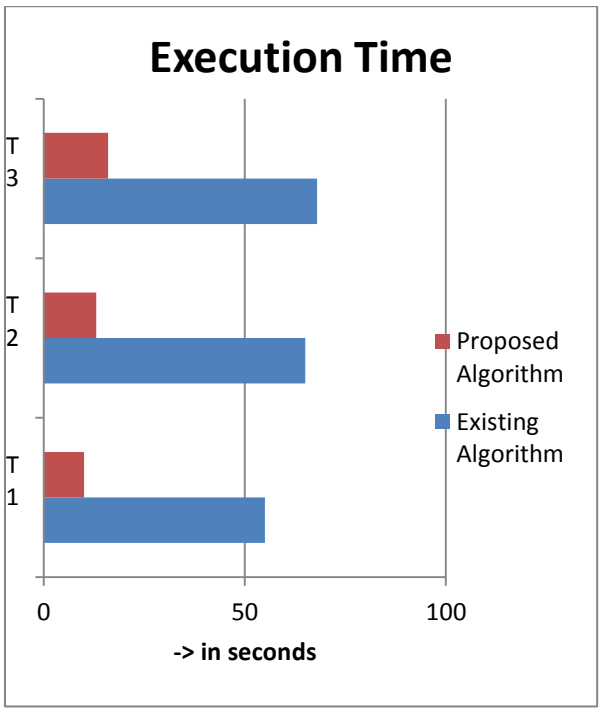

Fig 3: Execution Time Comparison

As shown in the figure 3, the execution time of the proposed technique is compared with the existing

technique. It is been analyzed that execution time of proposed algorithm is less as compared to existing technique.

Conclusion

The cloud computing is the architecture in which host, cloud server, virtual machine and brokers are involved in the communication. The cloud architecture is the decentralized due to which malicious hosts enter the network which are responsible to trigger various types of active and passive attacks. The zombie attack is the active type of attack in which malicious host spoofs the credentials of the legitimate host. The technique of mutual authentication is been proposed in this work which detect malicious hosts from the network. In the proposed technique, the hash functions are used to ensure the data integrity which is used to detect malicious nodes from the network. The performance of the proposed technique is analyzed in terms of space utilization, execution time, it is been analyzed that these parameters are optimized.

References

[1] Young-Gi Min "Cloud Computing Security Issues and Access Control Solutions", 2012, Journal of Security Engineering

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

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

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

[5] Simarjeet Kaur, "Cryptography and Encryption in Cloud Computing", 2012, VSRD International Journal of Computer Science and Information Technology, Vol. 2(3), 242-249

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

[7] Ivanov, Aleksei, "Side-Channel Attacks", 2005, IEEE, volume V, issue IV

[8] Ajey Singh, Dr. Maneesh Shrivastava, "Overview of Attacks on. Cloud Computing" 2012, semantic scholar, Volume 1, Issue 4

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

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

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

[12] Mohamed Saied Emam Mohamed, Stanislav Bulygin, Michael Zohner, Annelie Heuser, Michael Walter, Johannes Buchmann, "Improved Algebraic Side-Channel Attack on AES", 2011, IACSA

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