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

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.300 – 304

RESEARCH ARTICLE

To Propose A Novel Technique to Isolate and Detect Virtual Side Channel Attack in Cloud Computing

Pardeep Kumar [1], Jagdeep Kaur[2]

[1]Department of Computer Science, KCCEIT SBSNAGAR, India
[2]Department of Computer Science, KCCEIT SBSNAGAR, India
[1] pardeepk_88@yahoo.com; [2] Jagdeep.kaur@kcinstitutes.com

Abstract— Cloud computing is one of the most important technology of networking which is widely used in these days. Cloud computing has some security issue also. There are several types of attacks which can be launch on cloud very easily and has many serious effects on the network. This paper discussed the proposed scheme to overcome the adversary effects of virtual side channel effects.

Keywords— Private cloud, public cloud, virtual side channel attack

I. INTRODUCTION

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 [4] on these clouds is taken as a cloud application. 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. those services regardless of time and location [2]. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources like networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models".(Deyan Chen,2012).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 [12].Network security, information security and many other security types like the computer security together make the term "Cloud Security". Because it consist all of the security mechanism given above. It gives the broad set of technologies, policies and controls that are used to secure the data and applications exist with the cloud computing environment [13]. It is not the product of computer security like anti-viruses and anti-spam's. Security is the most concerning point to any service. External security or internal security required to each field. Only security ensures the privacy and integrity the cloud data. There are many security loopholes exist in the service. There are many types of security issues exist like DDOS, Man in the middle etc.

II. LITERATURE REVIEW

Punithasurya K (2013) in this paper a Novel Role Based Access Control technique is proposed[1] to enhance the security requirement of cloud data storage which is named as secure cross domain access control. Their proposed methodology maintains user's roles, permission and set of user attributes to create attribute ID for each user. The proposed access control method include of the ABAC , DRBAC and RBAC. This technique minimizes the time constraints issue and Location constraints issues. as we know Access control gives the authorization rights to the individual users. 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). Gouglidis Antonios (2011) introduced and describe the definition [2] 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. 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. Chen Danwei (2011) discussed cloud [3] 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. Ramadan Abdunabi(2008) presently [4] 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. Abdul Raouf Khan (2012) [5] 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. Bibin K Onankunju (2013) introduced [6] 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.

III. VIRTUAL SIDE CHANNEL ATTACK

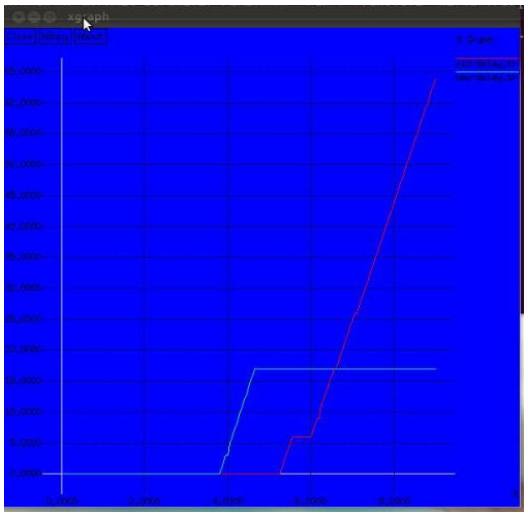
The one of the model of deployment IaaS provides infrastructure collection in cloud computing like virtual machines, multiple computers and number of resources to users to store their application, information, confidential of file, document information etc. With the help of Amazon E2 service it is possible to map the internal cloud infrastructure and to identify where the exactly target virtual machine reside in the network [7]. 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: Placement and Extraction [8]. 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. 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. Evaluating a cryptographic system's resilience to side-channel attacks is therefore important for secure system design. Authentication is a pathetic point in hosted and virtual services and is frequently targeted. There are many different ways to authenticate users and these are based on what a person knows. The mechanisms used to protected the authentication process and the method used are a common aim of attackers [9]. Now the architecture of SaaS, IaaS, and Paas, is only IaaS offer this type of information security and data encryption. If the transmitted data is categorized to secret for any project then the cloud computing service are based on IaaS architecture. This will be the most correct result for safe data communication. Moreover the authorization of data process or management for those data belonged to the enterprises but stored on the service provider's side must be approved by the user side (Halmen K.,2009).

IV. PROPOSED TECHNIQUE

The Cloud Computing Architecture of a cloud solution is the structure of the system, which comprises on-premise and cloud resources, services, middleware, and software components, geo-location, the externally visible properties of those, and the relationships between them [10]. The benefits of cloud computing are many. One is reduced cost, since you pay as you go. Other benefits are the portability of the application is that users can work from home, work, or at client locations. This increased mobility means employees can access information anywhere they are. There is also the ability of cloud computing to free-up IT workers who may have been occupied performing updates, installing patches, or providing application support. Along with the good services of Cloud Computing has to offer, there are security problems which make users anxious about the safety, reliability and efficiency of migrating to cloud computing. Big companies have second thought whether to move into the cloud because they might compromise the operation and the important information of the company. After analyzing and calculating the possible risk. Migrating into the "Cloud" will make computer processing much more convenient to the users. One of the considerations when moving to cloud is the security problems [11]. The legitimate user can access the data which is stored on the cloud. In the cloud computing, it is difficult to main the access control lists. The many techniques have been proposed for the access control. Among the entire techniques role based access control is the efficient and reliable technique for access control. In role based access control technique legitimate user can prove its identity to cloud service provider through the secure authentication procedure. According to user rights, the access is provided to the user. The main problem in such technique is security [12]. Many security attacks are possible in role based access control technique. The new technique is developed which is based on the identification and role based access control modals. This technique is the hybrid type of technique. In this technique the side channel attack is possible, In which attacker place the virtual machine and all the traffic of the legitimate user will directed to the attackers virtual machine. The attacker will hijack all the credentials of the legitimate user, and present it to server on the behalf of the legitimate user. In this paper we will enhance the "Role-Based Multi-Tenancy Access Control Scheme", to prevent the side channel attack.

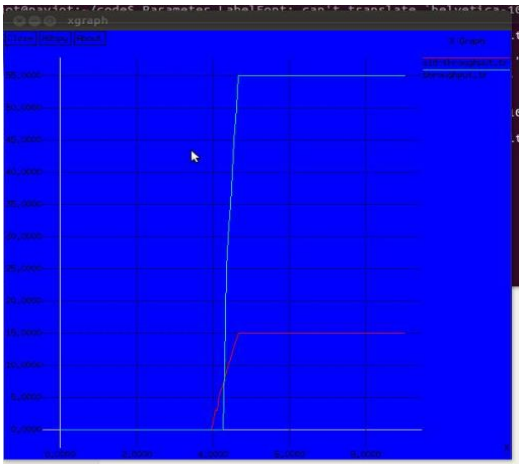
V. RESULTS

In above graph red line shows old delay and green line shows new delay. It concludes the proposed technique graph is better than existing graph.



Graph 1 of delay

In graph 2 red line represent old throughput and green line represent new throughput which is better than existing technique.



Graph 2 of throughput

VI. CONCLUSION

The main objective of this research paper is to discuss various attacks of cloud computing. We also focused on virtual side channel attack and its various advantages and disadvantages of the same. We believe that proposed algorithms discussed in this paper will give benefit for various research scholars. Its experimental results show that proposed technique gives better result which has better throughput and less delay as compare to existing techniques.

REFERENCES

[1] Bibin K Onankunju "*Access Control in Cloud Computing"* International Journal of Scientific and Research Publications, Volume 3, Issue 9 (2013).
[2] Gitanjali "*Policy Specification in Role based Access Control on Clouds*" International Journal of Computer Applications (0975 – 8887) Volume 75– No.1(2013) .
[3] Deyan Chen, "*Data Security and Privacy Protection Issues in Cloud Computing"* International Conference on Computer Science and Electronics Engineering (2012).
[4] Khan, A. R. "*ACCESS CONTROL IN CLOUD COMPUTING ENVIRONMENT*" *Journal of Engineering & Applied Sciences, 7*(5), (2012).
[5] Chen Danwei, Huang Xiuli, and Ren Xunyi "Access Control of Cloud Service Based on UCON" Nanjing University of posts & Telecommunications (2011).
[6] Gouglidis Antonios "*Towards new access control models for Cloud computing systems"* University of Macedonia, Department of Applied Informatics (2011).
[7] Gerald Kaefer "*Cloud Computing Architecture",* Corporate Research and Technologies , Munich, Germany, Siemens , Corporate Technology (2010) .
[8] Foster, I. Zhao, Y "*Cloud Computing and Grid Computing 360-Degree Compared"* In: Grid Computing Environments Workshop (2008).
[9] Ramadan Abdunabi and Indrajit Ray "*Extensions to the Role Based Access Control Model for Newer Computing Paradigms* (2008).
[10] Ning, G. jiamao, L. xiaolu, C "*Theory and Practice R & D of Web Services*" p. 10. Machinery Industry Press (2006) .
[11] Ning, G. jiamao, L., xiaolu, C (2006) "*Theory and Practice R & D of Web Services*" p. 10. Machinery Industry Press .
[12] Germany "*Rbac, role based access control 2000 workshop*" Berlin (2000).

