A Review of Virtual Side Channel attack in Cloud Computing Architecture

AMIT VERMA[1*], MEGHA MITTAL[1], BHARTI CHHABRA[2]
[1*]*Professor and Head, Department of Computer Science, CEC Landran, Mohali, Punjab*
[1]*M.Tech Research Scholar, Department of Ccomputer Science, CEC Landran, Mohali, Punjab*
[2]*Assitant Professor, Department of Computer Science, CEC Landran, Mohali, Punjab*

Abstract— Cloud computing is a leading distributed computing paradigm which provides convenient and on-demand network access to a shared group of computing resources like networks, servers, applications, storage and services that can be rapidly provided with minimum management and efficient requirement. Cloud is a centralized database where many clients /organizations accumulate their data and probably modify data and retrieve data. But there are various issues in the cloud computing that are being faced by organizations these days i.e. security, privacy etc. As more and more organization are moving to cloud computing, there are more chances of the data being hacked by the hackers/data criminals. Access control is usually a strategy or practice that allows, put a limit on access to a system. It may, as well, observe and trace all attempts made to use a system. It classifies the unauthorized user's tries to access the system. This process of controlling the user is quite important for the system. In this paper we have proposed to design a new technique to detect and isolate the virtual attack in cloud computing architecture. Our aim is to study and understand the existing techniques of detection and isolation of virtual attack and develop a new algorithm to detect and isolate the same in more efficient way on the basis of the throughput of the network.

Keywords: **-** Cloud Computing, Access control, Attacks in cloud computing, Virtual attack, Security Issues in cloud computing, cloud computing service models.

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 over the Internet are provided to the external customers [1]. Cloud is the network which is created through cloud service and computing model is the service provided in cloud.

Access control is one of the most important security mechanisms in cloud service, and the traditional access control model is not appropriate to achieve access control due to of its characteristics. But there may be cloud services required to face the same security issues and Security needs and however we can't be divorced from the traditional access control model ideas also. For Unauthorized Access issues they are often built on Delicate ID authentication and authorization. The primarily causes include: No authentication or weak authentication. For sending password and authentication information in plaintext, the system should adopt a strong authentication mechanism and make encryption communication to avoid unauthorized access. The three Cloud Computing Service models are:

SaaS: It is used as a distribution model which serves the free access of the software to the authenticated user over the same cloud.

PaaS: It is used as a distribution model which serves the free access of the platform for different software's to the authenticated user over the same cloud. (Java, python, .Net)

IaaS : Used to distribute processing, storage, networks, and additional necessary computing resources where the consumer is able to install and run random software, which can include operating systems and application[10].

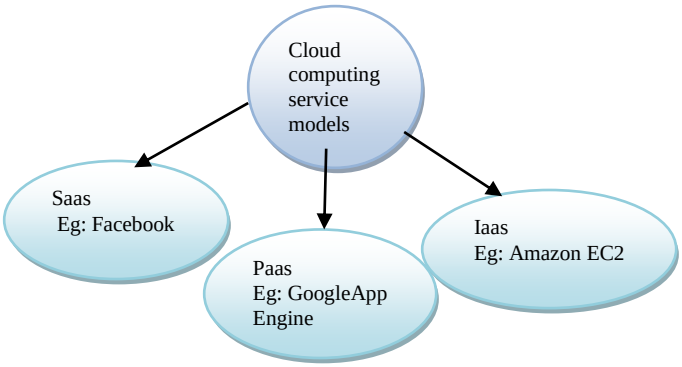

Fig.1: Service Models

There are several cloud deployment models that are distinguished on the basis of ownership of services provided to the organization and the physical location. The cloud computing deployment models are:

Public cloud – It is a type of cloud hosting in which the resources and cloud services are delivered to the general public over the network. Example: Google.

Private cloud –In private cloud, services are just available to a single organization comprising finite group of users. Private clouds can be internally or externally hosted.

Hybrid Cloud: Hybrid cloud is integrated type of computing. It is the combination of two or more cloud servers that can be private, public or both bounded together.

Community Cloud: It is a type of cloud which is jointly shared between various organizations that belong to some particular community, i.e. banks. It has cost saving capacity as the cost is shared by the specific organizations within the community. Community cloud is suitable for the organizations that work on joint ventures.

Cloud Computing Attacks

As more and more organization are moving to cloud computing, there are more chances of the data being hacked by the hackers/data criminals. There are many potential attack vectors that the criminals may attempt, such as:

a. Denial of Service (DoS) attacks: Security professionals have always argued that the cloud is more vulnerable to DoS attacks, because it is being shared by many users and that makes DoS attacks much more detrimental. When a Cloud Computing operating system notices a high workload on the flooded service, it starts providing more computational power to handle the additional workload which means that the server hardware boundaries (maximum workload to process) no longer hold. Which in turn means that the Cloud computing system is trying to work against the attacker, but it actuality to some extent it supports the attacker, by enabling him to do the most possible damage on the service's availability, starting from a single flooding attack entry point? Thus, the attacker doesn't have to flood all servers that are providing a certain service in target, but simply can flood a single Cloud-based address in order to create a total denial of service on that particular target server.

b. Virtual attacks: In a side channel attack, an attacker places the unauthorized virtual machine just near to the legitimate virtual machine being contacted and it then intercepts the calls being made to the legitimate machine. User trying to contact the legitimate virtual machine, sends all its credential to that unauthorized virtual machine as the user doesn't identify that it is a not the legitimate virtual machine. Attacker captures all the credentials and presents them to the legitimate virtual machine as an authorized user for hacking into it.

c. Authentication attacks: Authentication is a weak point in hosted and virtual services and it is frequently targeted by the attackers. There are various ways in which the user can be authenticated; for e.g., based on what a person has, knows, or is. The approaches that are used to secure the authentication process and the methods used for authentication are frequently targeted by attackers. Currently, among SaaS, IaaS, and Paas, only IaaS offers high level of information protection and data encryption. If the transmitted data is categorized as highly confidential, then the cloud computing service based on IaaS architecture would be the most suitable solution for secure data communication. In addition to this, the authorization of data process or management for the data belonging to the enterprise(s) but the data stored on the provider's side must be authorized by the users (enterprises) instead of the service provider's side. Most user-facing services are still using simple username and password type of knowledge-based authentication, with the exception of some financial institutions which have started deploying various other forms of secondary authentication systems (such as site keys, virtual keyboards, shared secret questions, otp etc.) to make phishing attacks a bit more difficult.

d. Man-in-the-middle cryptographic attacks: This is carried out when an attacker places himself between two users, i.e. between two communicating servers. If an attacker places himself between the communication paths, there is the possibility that they can intercept and modify communication being made.

e. Inside-job: These kind of attacks are carried out by a staff member or employee or whosoever is knowledgeable of how the system runs from client to server. In these kind of attacks the attacker (staff member) can implant malicious piece of codes which in turn damages any piece of data/information present on the cloud machine[10].

II. LITERATURE REVIEW

Keiko Hashizume, et.al [14] has proposed the analysis of various security issues in cloud computing architecture. They analysed the SPI model i.e SaaS,PaaS,IaaS vulnerabilities and threats . When information is provided all the way through internet or involvement of third party is there, at that time we have to ensure the security of the data and provide trusted security measures to organization. There is list of vulnerabilities and different threats relationship between them is also explained. Various virtualization technologies approach security mechanisms in different ways. The biggest security concerns in Cloud Computing are the storage capabilities and virtualization. Relation between security issues was not enough, so they have made relationship between vulnerabilities and threats to identify what vulnerabilities contribute to the execution of these threats and make the system more robust. Virtual networks are also target for some attacks especially when communicating with remote virtual machines. When any network in cloud computing architecture communicates with remote virtual machines, it is also target for some security attacks such as side channel attack and vulnerabilities. In this, they have discussed and analysed some of the vulnerabilities related to cloud computing.

Punithasurya K, et.al [11] has proposed a novel access control technique to improve the security issues of cloud data storage space which is named as secure cross domain access control. The proposed technique maintains the user's permission, roles and set of user attributes to create attribute ID for each user. The proposed access control method includes the ABAC, DRBAC and RBAC. The proposed methodology minimizes the time constraints and Location constraints issues to a great extent, as Access control provide the authorization and authentication rights to the users. Access control basically contains access privileges based on the user needs.

```
/* For achieving cross domain access */
/* For cross domain access consider set of domains for public sharing */
Domain A= { user n1, user n2, user n3….user nn }
Domain B= { user m1, user m2, user m3…user mn }
Domain C= { user p1, user p2, user p3…. user pn }
Roles = { Domain Manager, Domain Provider, Data owner }

Permissions = { R, W, RW }
For user n2 request resource in Domain A
{ if (user n2 attribute ID matches)
    { Data owner checks user n2 ID; //user n2 attribute ID has been stored in DO1
      Grants Access;
    Else
      Access forbidden; }
Else if (user n2 attribute not matches)
{ Data Owner checks for the user n2 roles & permission
  If (Authorized person in Domain A)
    { Domain A saying that Resource not available; } } }
/* Achieving cross domain access */
For user p1 request resource in Domain B
{ if( user p1's ID==TRUE)
   { user p1's ID available in Domain C;
     Domain C== user p1's ID;
     Domain B checks user ID in Domain Manager;
     Grant access to user p1;}
Else
   { Access forbidden; }}
```

Fig 1: Flow of Cross Domain Access Method

```
/* For Adding Data Security */
/* Adding ATTRIBUTE KEY GENERATION to make user identity secure */
For user m1's ID attribute
{ generate user m1 ID;
  Set of users m1's attribute -> Domain B; Attribute checks in Domain manager;
Now,
   Generate Random Value[unique] attribute = i; Generate Random value [ user ] = r;
   Secret key= (i+r).user m1's ID;
 }
/* Encrypting user data along with ID
 */ Encrypt ( user ID. (i+r)+data)
/* Decrypting user data along with ID
*/ Decrypt ( user ID. (i+r)+data)
```

Fig 2: Ensuring Security in Cross Domain

Gouglidis Antonios [5] has described and introduced the description of Cloud computing paradigm containing related concepts and characteristics**.** In this, they have applied the conceptual classification of computing models and described the list of associated characteristics. In result they foresee the applied methodology to instigate further research for the characterization of access control requirements in Cloud computing environments and furthermore to result in innovative access control models.

Chen Danwei, et.al [4] has discovered that the cloud service security is the major concern. Cloud service is mainly the web Services and it has various security issues including the security threats that are faced by the web services. The progress of cloud computing services strongly relates to security thus the further research of cloud computing service security is a significant matter. Initially, this paper give explanation about cloud computing and cloud services and then provides cloud services access control model that is based on UCON and negotiation techniques and also designs and implements the negotiation module.

Shucheng Yu [2] has described the security issue on one side by defining and imposing access policies that are based on data attributes and on the other side permitting the data owner to assign most of the computational tasks involved in fine-grained data access control to entrusted cloud servers without allowing them to access the underlying data contents. They accomplish this goal by exploiting and uniquely joining the techniques of attribute-based encryption (ABE), lazy re-encryption and proxy re-encryption. The proposed novel techniques have a relevant characteristic that is confidential user access privilege and the user's secret key liability. In result, they showed that the proposed technique is efficient and it provides security in cloud computing environment.

Md. Bajlur Rashid, et.al [10] has proposed an encrypted key generation algorithm against virtual side channel attack. Random key creation helps to encrypt information and decrypt from the similar encryption key. The methodology is that when a client store or maintain information in the cloud, random keys encrypt the data and change it during the encryption process. Although an invader can obtain this encrypted information from the cloud but he could not get any information about it. The encrypted data is afterwards decrypted using previous randomly generated key when the client executes any action to see the information.

Pseudo code for encryption operation:

1) Select two random numbers p and q
2) Read a plain text n
3) Calculate m = p*q+n
4) Calculate cp = 62-bitConvert (m)
5) Set cp as cipher text of n
6) Calculate k = (p*q) % n
7) Select upper closest prime and lowest closest prime of k as

p, q respectively
8) Repeat Step 2 to 7 until plain text remains

Pseudo code for decryption operation:

1. Read a cipher text cp
2. If separator is not true then go to next step otherwise go to step 4
3. Add cp in tempString and go to step 1
4. Generate two random numbers p, q
5. Get the decimal value of tempString as m
6. Calculate d as m-(p*q)
7. Add d as plain text
8. Make tempString Empty
9. Go step 1 if cipher text remains

III. RESEARCH METHODOLOGY

Access control is usually a strategy or practice that allows, put a limit on access to a system. It may, as well, observe and trace all attempts made to use a system. It classifies the unauthorized user's tries to access the system. This process of controlling the user is quite important for the system. There are many models or methods to control the access, which includes most common Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC). These control models are based on identity. Users (subjects) and resources (objects) are identified by unique names in these identity based models. Their identification can be done on the basis of the roles of subjects or directly. These access control methods are efficient in unalterable distributed system, where there are only a set of Users with a known set of services. The side channel attack is possible in RB-MTAC and it will lessen the network reliability and security of the system will be compromised. In this regard, we will enhance the Role based Multi-Tenancy Access control scheme. To prevent the side channel attack, novel technique will be proposed which is based on the server identification. Before presenting its identification to the server, officially recognized client will ask the server for its id. If the credentials are verified then further process will proceed, otherwise algorithm will stop. The proposed technique will be implemented in NS2 tool.

Context level data flow diagram depicts the plain view of mutual authentication scheme. It explain the process in which initially input is provided from the cloud service provider and after that it will detect the attack.

Level 1 shows the detailed process in which the cloud service provider will check both the user and the virtual machine and matches their respective addresses and then access is granted to them.

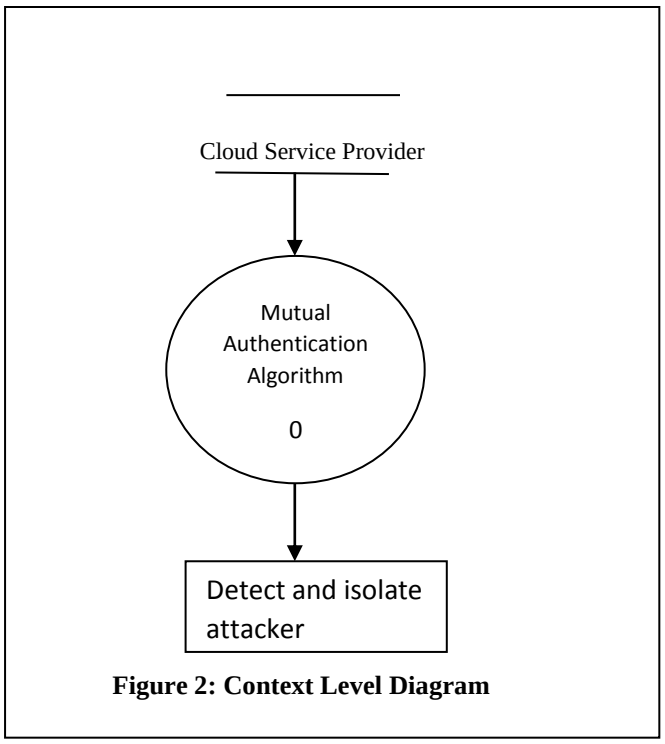

Figure 2: Context Level Diagram

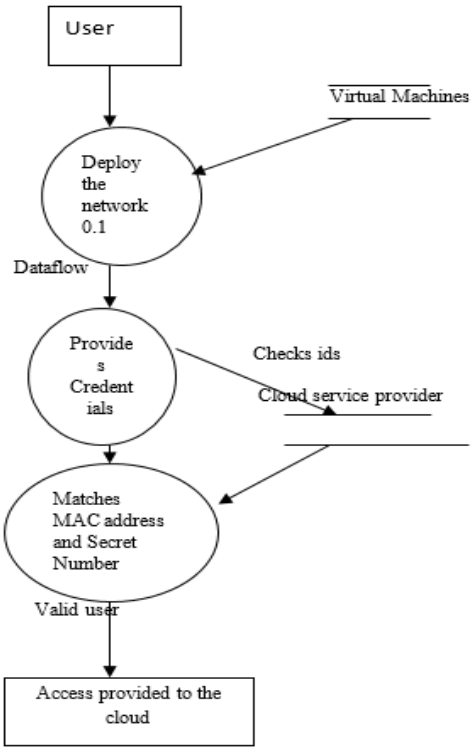

Fig.3: Level 1 diagram

IV. CONCLUSION

In this attempt, we have studied the key challenges of cloud computing and the various types of attacks in the cloud computing that can take place. In a side channel attack, an attacker places the unauthorized virtual machine just near to the legitimate virtual machine being contacted and it then intercepts the calls being made to the legitimate machine. It leads to the decline in the network reliability and also compromises its security. So we will focus on the detection of virtual attack and to isolate it by proposing a novel technique based on server identification.

V. REFERENCES

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

[2]. Shucheng Yu, Cong Wang, Kui Ren and Wenjing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", Conference on Information Communications, Page 534-542, 2010

[3]. Gerald Kaefer," Cloud Computing Architecture", Corporate Research and Technologies , Munich, Germany, Siemens , Corporate Technology, 2010

[4]. Chen Danwei, Huang Xiuli, and Ren Xunyi, "Access Control of Cloud Service Based on UCON", Nanjing University of posts & Telecommunications, Volume 3, No.4, pp 647-651, Nov 2009

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

[6]. Shantanu Pal, Sunirmal Khatua, "A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security", Annals of Faculty Engineering Hunedoara – International Journal Of Engineering, page 71-78, 2012

[7]. Abdul Raouf Khan, "Access Control IN Cloud Computing Environment", Journal of Engineering & Applied Sciences, Volume 7, No.5, pp 613-615, May 2012

[8]. Deyan Chen, Hangzhou, Zhejiang China, "Data Security and Privacy Protection Issues in Cloud Computing" International Conference on Computer Science and Electronics Engineering, Volume1, pp 647-651, March 2012

[9]. Reeja S L, "Role Based Access Control Mechanism in Cloud Computing Using Co - Operative Secondary Authorization Recycling Method" International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 10, pp 445-450, October 2012

[10]. Md. Bajlur Rashid, Nazrul Islam, et.al , " Randomly Encrypted Key Generation Algorithm Against Side Channel Attack in Cloud Computing", International Conference on Electrical Engineering and Information & Communication Technology, May 2015

[11]. Bibin K Onankunju, "Access Control in Cloud Computing", International Journal of Scientific and Research Publications, Volume 3, Issue 9, pp 31-33, September 2013

[12]. Gitanjal, Sukhjit Singh, "Policy Specification in Role based Access Control on Clouds", International Journal of Computer Applications, Volume 75, No.1, pp 39-43, August 2013

[13]. A Akinbi, E. Pereira, C. Beaumont,"Identifying Security Methods and Controls for Secure PaaS Cloud Environments" International Journal of Emerging Technology and Advanced Engineering, 2013

[14]. Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernande, "An analysis of security issues for cloud computing",Journal of Internet Services and Applications, February 2013