“Study of Virtual Side Channel Attack in Cloud Computing” A Review

Navjot Singh Brar, Dr Kanwalvir Singh Dhindsa
M.Tech (E-Security), Associate Professor
Department of Computer Science and Engineering
BBSBEC, Fatehgarh Sahib, Punjab, India

***Abstract*-Cloud Computing is the next generation Internet Service and data center used for public utilities and on-demand computing. Cloud computing is not a totally new technology, but rather a derived concept of application and service innovation in which, multi-tenancy is one of the important issues among the core technologies of cloud computing applications. Many tenants can access the different applications and computing resources in the same cloud server, whereas concurrent use by many users on a database or application will lead to large data volume, time consuming and security issues. Under these circumstances, it is particularly important to separate application and data for conflicts avoidance to enhance the system and data security. In this research work we study various key challenges of cloud computing and identify the various access control schemes for cloud computing. This paper emphasizes the cloud service model under a Multi-Tenant Architecture (MTA), using identity management and Role-Based Access Control, to enhance a Role-Based Multi-Tenancy Access Control (RB-MTAC).Side channel attack is possible in RB-MTAC.To prevent the side channel attack; a technique will be proposed which is based on the server identification. Before presenting its credentials to the server, legitimate client will ask the server for its credentials. If the server’s credentials are verified by the client then further process will proceed otherwise algorithm will halt. The proposed scheme is compared with the existing scheme.**

***Keywords*- MTA, RB-MTAC, SLA tenant, SaaS, PaaS, IaaS.**

1. INTRODUCTION

1.1 Cloud Computing

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. 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. Cloud computing is use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams.

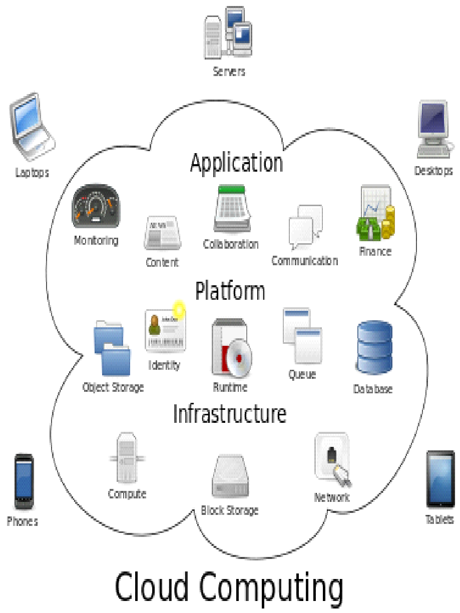

Figure 1: Cloud Computing Architecture [19]

It is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. The data in a Cloud is stored on to centralized location called data centers having a large size of data storage. The data as well as processing is somewhere on servers. So, the clients have to trust the provider on the availability as well as data security. The SLA is the only legal agreement between the service provider and client [9]. The basic principle of Cloud computing is to distribute the computing tasks to many distributed computers, not local computer or remote servers.

Cloud computing architectures can be either public or private. A private cloud is hosted within an enterprise, behind its firewall, and intended only to be used by that enterprise. In such cases, the enterprise invests in and manages its own cloud infrastructure, but gains benefits from pooling a smaller number of centrally maintained high-performance computing and storage resources instead of deploying large numbers of lower performance systems [5]. Further benefits flow from the centralized maintenance of software packages, data backups, and balancing the volume of user demands across multiple servers or multiple data center sites. In contrast, a public cloud is hosted on the Internet and designed to be used by any user with an Internet connection to provide a similar range of capabilities and services.

Access control is one of the most important security mechanisms in cloud service, and Cloud service can not apply the traditional access control model 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 mainly causes include: No authentication or fragile authentication: to send the password and authentication information in plaintext. The system should adopt a strong authentication system and make encryption transmission to prevent unauthorized access [4].
The three service models are:

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

SaaS: In this model cloud service providers install and operate application software in the cloud and cloud users access the software. Some type of cloud based applications software like desktop as a service and communication as a service. eg. Facebook.
PaaS **:**In this type of cloud service model, cloud service providers delivers a computing platform like operating system, programming language execution environment, database and web server (Java, python, .Net). eg. GoogleApp engine.
IaaS: This is the most basic cloud service model, providers offer computers as physical or more virtual machine and other resources. The virtual machines are run as guests by virtual machine manager or monitor [9].eg. Amazon EC2.

1.1.2 Comparison of SaaS, PaaS and IaaS

The comparison between three service models is as follows:

	SaaS	**PaaS**	**IaaS**
Description	A complete application as a service on demand.	An application development and deployment platform	Hardware and associated software
Advantages	Reduced operating expenses	Reduced cost and complexity of buying and managing tools.	High flexibility, low cost, access to latest technology
Examples	Facebook	GoogleApp engine	Amazon EC2

Table1: Comparison of three Service Models

1.2 Cloud Computing Attacks

There are many types of security issues in cloud computing. Due to these issues, attacks are possible in cloud. There are various potential attack vector criminals may attempt such as:
a. 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 .
b. Side Channel attacks – An attacker could attempt to compromise the cloud through placing a malicious virtual machine in close proximity to target the cloud server and then exploiting a side channel attack.

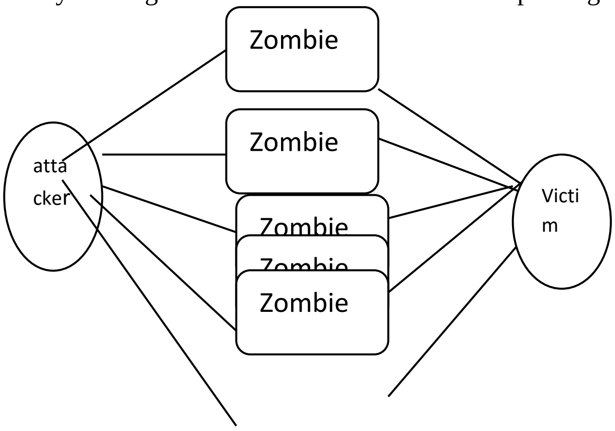

Figure 2: DDOS attack [20]

c. 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.

d. 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 gets between the receiver and sender 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.

Fig. 3 is an example of how a man-in-the-middle attack works. The attacker intercepts some or all traffic coming from the client and collects the information and then proceeds it to the destination the user was originally intending to visit.

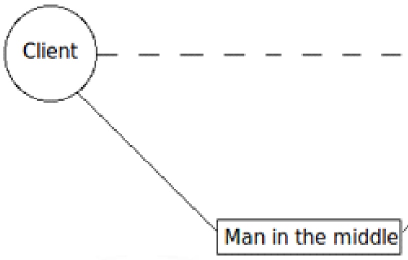

Figure 3: Man in the middle attack [21]

e. Inside-job – These kind of attack is when the staffs, person or employee or who is knowledgeable of how the system runs from client to server then he can implant malicious codes to damage everything in the cloud system[9].

1.3 Access Control, Authentications and ID Management

Access control is concern with key because insider attacks are on top risk. A potential hacker is one who has been entrusted with approved access to the cloud. Anyone considering using the cloud requires to look at who is managing their information and which types of controls are applied to these individuals. The traditional system of application centric access control in which each application keeps track of its collection of users and manages them which is not feasible in cloud based architectures . Because the user space maybe shared across applications that can lead to data storage replication and making mapping of users and their privileges a herculean task. It also needs the user's to remember multiple passwords /accounts and maintain them [3].

Cloud needs a user centric access control where every user request to any service provider is bundled with the user id and entitlement data information. User id will have attributes or identifiers that find and define the user. The id is tied to a domain but it should be portable. User centric technique leaves the user with the ultimate control of their digital ids[4]. User centric scheme also implies that the system maintains a context of information for every user in order to find how best to react to in a given situation to a given user request.

There should be a strong Identity Management and authentications or both the client and cloud provider . Access monitoring is to implement Key Management for both the cloud service provider and client . That Key must be known for both entities and will be remotely monitored. Server logs must be kept and Intrusion Detection ,Prevention System should be deployed for providing trust to the cloud computing provider that they kept the data well that is to avoid data leakage, there must be a shared key for both client and the provider. In order for the clients to access the cloud computing services it must be first authenticated, not only using a mere username and password but a digital ID's[17] .

1.3.1 Access control characteristics in the Cloud

In order to appoint a series of characteristics regarding access control we use the conceptual categorization for Cloud system [7]. There are four layers of the conceptual categorization. The entropy layer the type of shared objects within the boundaries of the entropy layer. The management layer defines needs from policy management and the logic layer incorporates requirements which identifies requirements from the dispersion of the objects in a system and the assets layer from is not handled by the former layers. A set of requirements for access control systems that are considered important for the Cloud infrastructure .

The identification of the requirements incorporates also characteristics that are exposed by the three levels of the information security infrastructure in the Cloud viz. application network level, level and host level where applicable. These characteristics may vary depending on the use cases that need to be supported by a specific system [16].

2. RELATED WORK

Yang and Lai[14] emphasized the cloud service model under a multi-tenant architecture(MTA) ,using identity management and role based access control,to propose and design a role-based multi-tenancy access control(RB-MTAC).The RB-MTAC apply identity management to determine the user's identity and applicable roles, since different users possess different functional roles with respective privileges for processing.

Antonios[7] describe 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.

Danwei [4] mainly discussed cloud service security. Cloud service is based on Web Services and it will face all kinds of security issues including what Web Services face. 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.

Abdunabi and Ray [10] presented 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 RBAC.

Khan [1] discussed various features of attribute based access control scheme suitable for cloud computing environment. 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.

Onankunju [3] introduced a new technique for providing secured access control in cloud storage. . 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.

Yu [15] described challenging open issue by on one hand defining and enforcing access policies based on data attributes and on the other hand allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. They achieve this goal through exploiting and uniquely joins techniques of attribute-based encryption (ABE), lazy re-encryption and proxy re-encryption.

Pal and Khatua[13] focused 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. Moreover this research aims towards proposing a new trusted and collaborative agent-based two-tier framework, titled WAY (Who Are You?) to protect cloud data resources. The framework can be used to provide security in infrastructure, network as well as data storage in a heterogeneous cloud infrastructure . If the trust updating policy is based on network activities then the framework can provide network security. Similarly it provides storage security by monitoring unauthorized access activities by the Cloud Service Users (CSU).

Akinbi et al.[2] discussed security requirements for identity and access management 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.

3. TYPES OF MODELS

Along the good services that Cloud Computing offers, 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. In the cloud computing, it is difficult to maintain the access control lists. Many techniques have been proposed for the access control. Various access control models are in use:

1. Mandatory Access Control(MAC)
2. Discretionary Access Control(DAC)
3. Role Based Access Control(RBAC)

All these models are known as identity based access control models. In all these access control models, user (subject) and resources (objects) are identified by unique names. Identification may be done directly or through roles assigned to the subjects .These access control methods are effective in unchangeable distributed system, where there are only a set of users with a known set of services.

1. ***Mandatory Access Control (MAC)***-MAC model counter threats by controlling access centrally. An ordinary user cannot change the access right a user has with respect to a file and once a user logs on to the system the rights he/she has are always assigned to all the files he/she creates.MAC policy decisions are based on network configuration. Only administrator can assign permission to access objects and subjects. Administration defines the access policy and usage which cannot be modified or change by the user.

Advantages:

1. MAC policy decisions are based on network configuration.
2. MAC is the main access control model used by the intelligence agencies and military policy access restriction.

2. Discretionary Access Control (DAC)-DAC is a user centric access control model, that a file owner determines the permissions that are assigned to other user requiring access to the file. There is no central control, so this method is easy to implement in a distributed application on the web.

Advantages:

1. This model is easy to implement because there is no central control in this model.
2. This model is based on the resource ownership.
3. DAC is controlled by the root/administrator or owner rather than being hard coded into the system.

3. Role-Based Access Control (RBAC)-MAC and DAC proved to be problematic for distributed systems and managing the access to resources and system become hard so new access model is introduced , known as a role-based access control model. In this, permissions are associated with roles and users are assigned to appropriate roles. Three primary rules are defined for RBAC:

1. Role Assignment: A subject can exercise permission only if the subject has selected or been assigned a role.
2. Role Authorization: A subject's active role must authorize for the subject. With rule1 , this rule ensures that users can take on only roles for which they are authorized.
3. Permission Authorization: A subject can exercise permission only if the permission is authorized for the subject's active role.

Advantages:

1. RBAC model defines set of basic RBAC elements(i.e. users ,roles, permissions, operations, objects)
2. RBAC models are more flexible than DAC and MAC.
3. A user can have more than one role and more than one user can have the same role.

4. CONCLUSION

Following table describe the various attributes of MAC, DAC and RBAC models. With the help of table we can easily understand the difference between these three identity based access control models.

	MAC	DAC	RBAC
Flexibility	Less	less	Higher
Role defined	Less	less	More
Ease of use	Difficult	easy	Difficult
Drawback	Only administrator can assign permission	Don't recognize human and computer program	Skilled personal are require
Scalability	Less	less	Higher
Used by	Intelligence agencies	In smaller companies	In bigger companies

Table 2: Difference between three access models

RBAC model is more flexible than MAC and DAC because in RBAC users can assigned several roles and roles can be assigned to several users while in MAC only administration can assign permission to access objects and subjects. Administration defines the access policy and usage which cannot be modified or change by the user.

In RBAC a user can have more than one role and more than one user can have the same role, in DAC file owner determines the permission while in MAC administration can assign the permission.

DAC model is easy to use because there is no central control in this model. RBAC model is more scalable as compare to MAC and DAC model. As the organization grows more roles are needed which is only possible in RBAC.

MAC is mainly used by intelligence agencies and military policy access restrictions because security is the main issue and due to hard coding MAC is used. DAC is used in small organizations where work output is small and RBAC is used in large organizations because productivity is the main issue.

These models has drawback also. Drawback of MAC model is that only administrator can assign permissions to access objects and subjects. Policy defined by the administrator cannot modify by the user. In DAC model, main drawback is that they fail to recognize the difference between computer program and human user. While in RBAC model very skilled persons are required to implement the model.

REFERENCES

[1] Abdul Raouf Khan May 2012. "Access Control in Cloud Computing Environment", ARPN Journal of Engineering and Applied Sciences, Vol. 7, No.5, pp.613-615.

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

[3] Bibin K Onankunju, Sep 2013. "Access Control in Cloud Computing", International Journal of Scientific and Research Publications, Vol. 3, No. 9.

[4] Chen Danwei, Huang Xiuli, Ren Xunyi, Nov 2009. "Access Control of Cloud Service Based on UCON", Nanjing University of posts & Telecommunications, Vol. 3, No. 4, pp.559-564.

[5] Deyan Chen, Hong Zhao, March 2012. "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering, Vol. 1, pp.647-651.

[6] Gitanjali, Sukhjit Singh Sehra, Jaiteg Singh, Aug 2013. "Policy Specification in Role based Access Control on Clouds", International Journal of Computer Applications, Vol. 75, No.1.

[7] Gouglidis Antonios, 2011. "Towards new access control method in cloud computing systems".

[8] Ian Foster, Yong Zhao, Shiyong Lu, Ioan Raicu, Nov 2008. "Cloud Computing and Grid Computing 360-Degree Compared", Grid Computing Environments Workshop in University of Chicago.pp.12-16.

[9] Ling Li, Lin Xu, Jing Li, Changchun Zhang, Dec 2011. "Study on the Third party audit in cloud storage service", International Conference on Cloud and Service Computing, Hong Kong, pp. 220-227.

[10] Ramadan Abdunabi and Indrajit Ray, 2008. “Extensions to the Role Based Access Control Model for Newer Computing Paradigms”.

[11] Ravi Singh Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman, Feb 1996. “Role-Based access control models”, IEEE Computer, Vol. 29, No. 2, pp.38-47.

[12] Reeja S L, Oct 2012. “Role Based Access Control Mechanism in Cloud Computing Using Co - Operative Secondary Authorization Recycling Method”, International Journal of Emerging Technology and Advanced Engineering, Vol. 2, No. 10, pp. 444-1

[13] Shantanu Pal, Sunirmal Khatua, Aug 2011. “A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security”, pp.71-78.

[14] Shin-Jer Yang, Pei-Ci Lai, July 2013. “Design Role-based multi-tenancy access control scheme for cloud services”, Biometrics and Security Technologies, Chengdu, Vol. 13, pp. 273-279.

[15] Shucheng Yu, March 2010. “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing”, Vol.18, No. 4, pp. 534-542.

[16] Sonam Chugh, Sateesh Kumar Peddoju, May 2012. “Access control based data security in cloud computing”, Vol. 2, No. 3, pp. 2589-2593.

[17] Wei-Tek Tsai, Qihong Shao, March 2011. “Role based access control using reference ontology in clouds”, Conference: International Symposium on Autunomous Decentralised Systems (ISADS), Tokyo and Hiroshima, pp.121-128.

[18] Yinqian Zhang, Ari Juels, Alina Oprea, Michael K. Reiter, May 2011. “Home Alone: Co-residency detection in the cloud via side channel analysis”, Security and Privacy (SP) Berkeley, USA, pp.313-328.

[19] http://www.brighthub.com/environment/greencomputing/articles/127086.aspx#imgn-0

[20] http://www.betterhostreview.com/ddos-attack-protected-hosting.html

[21] http://www.ai.rug.nl/mas/finishedprojects/2011/TLS/hermsencomputerservices.nl/mas/mitm.html