Enhance Role Based Multi-Tenancy Access Control List to Protect Side Channel Attack

Jaswinder Kaur
ME Scholar, CSE Department
Lovely Professional University
Jalandhar, India

Kamalpreet Singh
Assistant Professor, CSE Department
Lovely Professional University
Jalandhar, India

***Abstract*- Cloud Computing enables on online access of resources and services from the pool of available resources on demand through internet. These resources and services are provided rapidly by CSP(Cloud Service Provider) to the users with minimum cost and with minimum level of effort because users need to pay as per they use resources and don't need to install them . Data and services in the cloud are distributed at different servers but user only sees the virtual view when they request for services. Easy access to the internet increases threat and possible attacks on Cloud services thereby increasing security concerns online. Cloud uses access control list for authenticate the legitimate users. The traditional access control has the security problems for such as Denial of service, Side Channel Attack etc. Multiple users can access the different applications and services on the same Cloud Server at same time. To avoid the conflicts in data and applications of different users Cloud uses the Role Based Multi-Tenancy Access Control List which enhances the security of Cloud. The dedicated id is assigned to each user for authorized access of cloud. RB-MAC does not protect from side channel attack because RB-MAC does not check for the authenticity of a virtual machine. This paper gives the brief over view of access list, RBAC, RB-MAC, side channel attack.**

Keywords: Cloud Computing; RBAC; RB-MAC.

I. INTRODUCTION AND RELATED WORK

Access Control List [1] assigns privileges to the users. In order to explain the Access Control List in detail lets refer the conceptual categorization of access list for Cloud Systems. In the conceptual Model there are four layers: Entropy layer which is the first layer from below identifies the requirements and second layer is Asset layer identifies resources from the shared resource pool according to the requirements identified by Entropy layer. Management layer is responsible for management of all the policies.

Logic layer handles all the requirements which are not taken care by other layers for example quality factor. Users interact through Entropy layer. In Access control list unique id is provided to each user and through that id access is assigned to the users [2].

Role Based Access Control (RBAC) has two phases for assigning a privilege to a user[3] As shown in figure 2 , In first phase, one or more roles are assigned to the users.

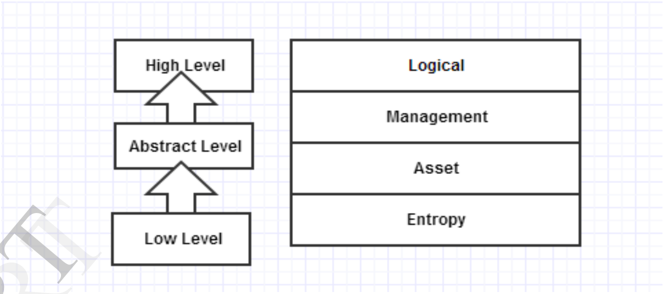

Figure1: Conceptual model

II. ROLE BASED ACCESS CONTROL LIST

In the second phase validation for roles is performed, to check whether the roles are authorized for the requested services or not. In the RBAC (Role Based Access Control List) permissions are assigned to roles not to the users. Roles can be in the hierarchical structure.

In the Role Based Access Control List all the permissions are assigned to roles, users need to be the member of roles for authorization process.

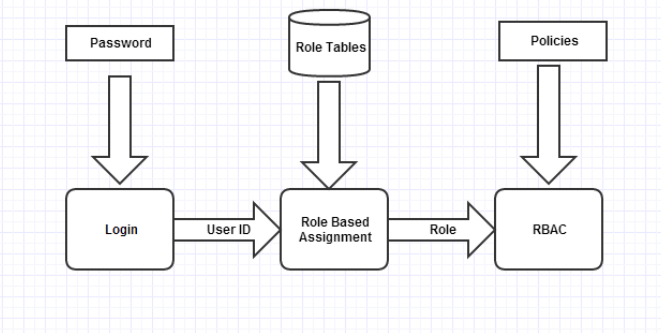

Figure 2: Phase Role Based Access Control Model

Users can access resources through roles. Users can register for particular role and on the bases of that assigned role resources are provided to the user and accordingly users can operate them. Roles make the management process easy because a role can have a large set of related authorizations. The authorization is not directly granted to the users , whenever the user required certain authorization he needs to first prove its authority for the role. In Role Based Access Control List all the decisions are made on the basis of access control list as it is discussed above. Role based Access Control principle include: separation of duties, data abstraction and least privilege[4].

RBAC comprise a family of four references models:

A. RBAC0: contains the core concepts of the Model. It is the minimum requirement for any system that exploits features of RBAC(Role Based Access Control Model).

Users permissions (P), user (U) , roles (R) and are three sets of entities and the relations between these entities are defined by Permission-Role Assignment and User-Role Assignment[5] . These sets and relations are the main concepts of the RBAC (Role Based Access Control Model). One user can register for more than one role and for one role there can be several numbers of members. A user can call multiple sessions within a session a user can invoke set of roles but each session related to only one user. One role can have multiple permissions and one permission can be the member of many roles.

B. RBAC1: adds to RBAC0 a role hierarchy (RH). Role hierarchies are an important concept for structuring roles to represent organization users responsibly and degree of authority.

C. RBAC2: introducing the concept of constraints. RBAC (Role Based Access Control Model) adds dynamic (related to sessions) and static (not related to sessions) constraints between core concepts[5].These constraints are considered to be the principle motivation for RBAC (Role Based Access Control Model) because constraints are powerful technique to lay out higher-level organizational mechanism[5]. Constraints can be applied to Permission-Role Assignment ,User-Role Assignment and session.

D. RBAC3: It includes all aspects of RBAC0, RBAC1 and RBAC2 and it is called a united model of RBAC).

RBAC3 combine RBAC1 and RBAC2 to combine both constraints role hierarchy .In these model constraints can be applied to the role hierarchy in addition to the constraints in RBAC2.

III. AUTHORIZATION CHALLENGES

1. User population is astir and the identities of all users are not always known in advance. Classical is not capable for supporting systems that provide services to unknown users. This is because RBAC needs users to be authenticated for access control. When users are dynamic and their identities are unknown determining users' authorization is challenging.

2. Some functions might be limited or periodic temporal duration. Traditional RBAC does not have temporal support. It has no provision for role activation during specified temporal intervals.

3. Users can give all or part of their authority to another user. This needs support for delegation as well as revocation of delegation neither of which are provided by traditional RBAC.

4. A user's context determines what actions can be performed in the system. Context typically is application dependent. Traditional RBAC components are limited to user, role, permission and constraint. There is no support for incorporating contextual information such as location or other environmental conditions in the model.

5. A system needs to collaborate with other systems to provide some services. RBAC is intended for a security control under a single administrative domain. Challenges that arise from collaboration like policy reconciliation or support for ad hoc policies are beyond the scope of RBAC[4].

RBAC under the multi-user environment is considered as RB-MAC [6] (Role Based Multi Tenancy Access Control). It combines the identity management and RBAC both as shown in figure 3. It firstly checks for the user identity then provide roles to valid users.

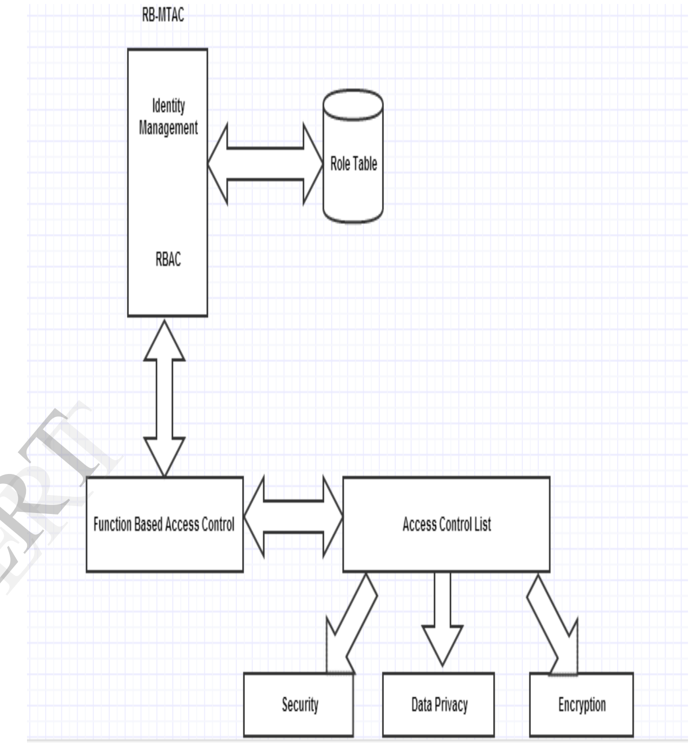

Figure 3: RB-MAC system structure

IV. SIDE CHANNEL ATTACK

In side channel attack attacker places the unauthorized virtual machine just near to the legitimate virtual machine[8]. User sends all its credential to that unauthorized virtual machine because user does not know the fact that it is a not the legitimate virtual machine. Attacker captures all the credentials of user and presents them to the legitimate virtual machine as an authorized user. RB-MAC does not protect from side channel attack as RB-MAC only checks whether the user is authorized or not. It does not verify that the virtual machine is legitimate or not. RB-MAC can be enhanced to protect from side channel attack if the mechanism of virtual machine authentication will be added into it.

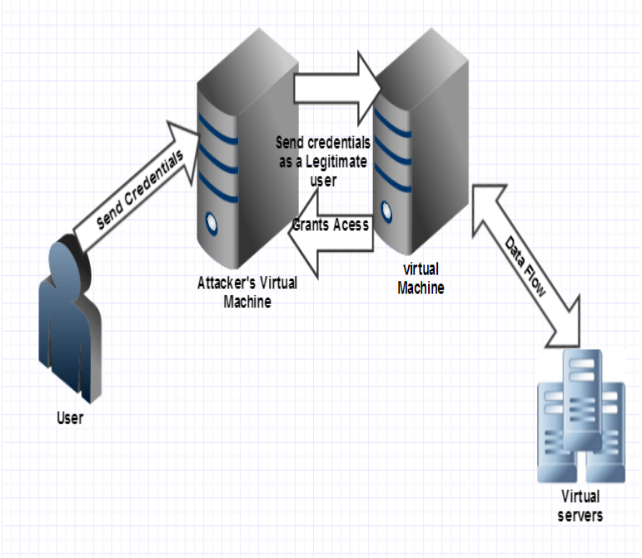

Figure 4: Side Channel Attack

V. CONCLUSION

Cloud Computing is a field of computer science in which user can access resources remotely through browser. As the data is stored on cloud user has lost the control over data once it is stored on cloud. So security of cloud is major issue in now days. As we discussed above to manage lots of id's in Access List is a major task and RB-MAC list provides the solution for the same .In which permissions are not assigned to users , permissions are assigned to roles in multi user environment. This provides a better solution for security issues in cloud. But RB-MAC does not protect from side channel attack , so to make the cloud more secure RB-MAC can be enhanced to provide protection from side channel attack. RB-MAC can protect Cloud from the side channel attack if it will check for the authentication of virtual machine also.

VI. REFERENCES

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

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

[3]. Germany, (2000)"Rbac, role based access control 2000 workshop," Berlin.

[4]. Gitanjali (2013)" Policy Specification in Role based Access Control on Clouds" International Journal of Computer Applications (0975 – 8887) Volume 75– No.1.

[5]. R. S. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman (1996), "Role-Based Access Control Models", *IEEE Computer* 29(2).

[6]. Shin-Jer Yang, Pei Ci Lai, Jyhjong Lin,(2013),"Design Role-Based Multi –Tenancy Access Control Scheme for Cloud Services",IEEE.

[7]. Deyan Chen, (2012)"Data Security and Privacy Protection Issues in Cloud Computing" International Conference on Computer Science and Electronics Engineering.

[8]. Qiasi Luo1 and Yunsi Fei2 "Algorithmic Collision Analysis for Evaluating Cryptographic System and Side-Channel Attacks", International Symposium on H/w- Oriented Security and Trust, 2011.