The Survey Paper on Cloud Security using RBAC model

Niranjan S J[1], Girish Deshpande[2]

[1]Assistant professor , Dept. of CSE, KIT,Tiptur-572202
[2] Assistant professor , Dept. of CSE, GIT,Belgam-590008

Abstract: *Cloud computing is a fast growing technology. In cloud computing, computing resources are provided as services over the Internet and users can access resources on based on their payments. This paper we discusses cloud security risks, with a focus on access control. As a traditional access control mechanism, role-based access control (RBAC) model can be used to implement several important security principles such as least privilege, separation of duties, and data abstraction. We argue that RBAC is well suited to many situations in cloud computing where users or applications can be clearly separated according to their job functions.*

Keywords – *Cloud computing, cloud security, Role-Based Access Control (RBAC).*

1. INTRODUCTION

The developing prevalence of distributed computing impacts each part of the data innovation (IT) industry [1]. It brings business nimbleness and lower costs for data frameworks by utilizing virtualization and shared foundations. By using existing access control models, cloud suppliers are able to control client exercises inside a solitary occupant.

Distributed computing gives on request assets to capacity to clients which can diminish the weight of specialist co-ops with respect to support costs. Additionally, distributed storage gives a flexible and fitting route for clients to get to their information from anyplace, whenever and on any gadget. Distributed computing has quickly changed the best approach to efficiently give the figuring and programming administrations to the customers on request. Cloud benefit demonstrate [2] can be sorted as: Iaas, PaaS and SaaS as appeared in figure 1. In Software as a Service (SaaS) cloud supplier gives the applications over the system which can be utilized by the cloud clients, Platform as a Service (PaaS) gives the earth in which clients make and convey their applications and Infrastructure as a Service (IaaS) gives the capacity, arrange ability to their clients on request.

For the most part three vital security ideas identified with cloud:

Fig. 1: Cloud Service Model

2. SECURITY RISKS FOR CLOUD PROVIDERS

Security chances in distributed computing situations include customary ideal models in data security, for example, classification, respectability, and accessibility (now and again alluded to as the CIA set of three). Be that as it may they have logical attributes in distributed computing. For instance, for most administration models, the security is to a great extent the obligation of the cloud suppliers. It is then fundamental to recognize hazard issues looked by the virtualized frameworks. These issues incorporate the accompanying [4].

- Complexity of configuration. Due to more complex usage of networks and systems, the possibility of improper configuration may increase. Such information may not be aware to consumers until some security incidents happen.

- Privilege escalation. An attacker may take advantage of different levels of access controls of Virtual Machines (VM) and escalate its access privileges through the use of hypervisor – a virtual machine monitor/controller that facilitates hardware virtualization and mediates all hardware access [4].

- Inactive virtual machines. Data stored in inactive virtual machines may contain sensitive information and has the potential to be accessed by unauthorized users.

- Segregation of duties. Since a VM provides access to different components using different mechanisms, properly identify access roles and segregate their duties could be difficult.

- Poor access controls. A hypervisor is basically a single point of access. It has the risk of exposing trusted network resources through poorly defined access control systems.

Access control is the process of limiting access to system resources for only authorized people, programs, processes, or other system components. Access control is one fundamental aspect of information security, and directly ties to the three aspects of the information security triad. From the perspective of access control, cloud computing providers should provide the following basic functionalities [5].

- Control access to the cloud service's features based on policies specified by the customer, and the level of service purchased by the customer.

- Control access to one consumer's data from other customers in multi-tenant environments. Also control access to both regular user functions and privileged administrative functions.
- Keep user profile information and access control policy accurate.
- Provide optional notification of account creation and removal.
- Provide adequate liability/audit logs on consumer and service provider activities. This seems important in the context of the previous discussion on the mutual auditability problem.

These functionalities can likewise be seen in get to control instruments for customary IT anticipates. To implement get to control, it has been said that all the accompanying customary models can be utilized as a part of distributed computing: required access control (MAC), optional access control (DAC) (for instance, get to control records or ACLs), and nondiscretionary get to control (for instance, RBAC or assignment based access control) [3][5]. The utilization of a model is very particular to cloud suppliers. It ought to be noticed that there are unique security suggestions because of the utilization of single sign-on (SSO) in distributed computing. SSO is a component that one client gives an ID/secret key combine (or other character data, for example, biometric highlights or advanced authentications) per work session, and is then naturally conceded access to all the required applications. Despite the fact that this appears to be helpful to purchasers, it makes a solitary purpose of disappointment that might be exceedingly vulnerable to outside assaults.

We contend that RBAC is a customary access control demonstrate and might be very much adjusted to a few circumstances in distributed computing, particularly in circumstances where clients or applications are obviously distinguishable as indicated by their activity capacities. We will proceed with the exchange with a formal definition and an UML portrayal on RBAC, trailed by its potential use in distributed computing. In spite of the contentions in the group, this paper means to center around the entrance control part of cloud security, and give an assurance instrument in light of the Role Based Access Control (RBAC) show. The utilization of RBAC in distributed computing and database frameworks isn't new; however in this paper we mean to utilize security examples to demonstrate the refined instrument. We additionally distinguish a few imperative elements in distributed computing at a refined level so that the RBAC could be instantiated.

3. ROLE-BASED ACCESS CONTROL (RBAC)

RBAC models can be utilized to actualize three vital security standards: minimum benefit, division of obligations, and information reflection [6]. The rule of slightest benefit implies that parts just have the base access rights required in a day and age. The second standard, detachment of obligation, implies get to consents are isolated among parts to encourage the administration of various security levels. Information reflection implies conceptual information get to authorizations rather than a straightforward arrangement (for instance, read, compose, and execute), can be set up in this model [6] .

RBAC is not the same as Discretionary Access Control (DAC). Access control in the RBAC show depends at work elements of clients. Clients have no privilege to pass their consents to different clients at their tact, as that in the DAC display. RBAC can be seen as a type of Mandatory Access Control (MAC) without multilevel security prerequisites [6]. The RBAC demonstrate has been connected in an assortment of certifiable administration frameworks. Other than its customary use in database frameworks, Bacon et al. at the University of Cambridge connected a RBAC framework called OASIS to accomplish interoperation in an open and disseminated condition [7]. Ferraiolo et al. at the National Institute of Standards and Technology (NIST) connected an improved RBAC model to arrange Web servers [6]. There are likewise different frameworks created for the keeping money group, organize applications, and superior bunch figuring conditions [12]. It has been recognized in the writing that database activities, for example, exchange preparing administrations, might be best served by RBAC models, perhaps supplemented by information driven strategy executed in hidden databases [5]. In this paper, we mostly take after the instrument depicted in [12]. The RBAC display instrument has turned out to be a valuable access control technique. Since distributed computing has close associations with different fields, for example, bunch/superior figuring and system applications, it is normal to expand the model in distributed computing.

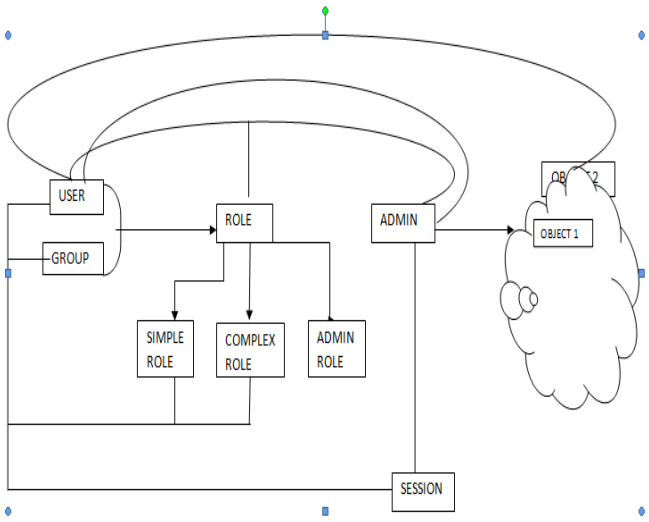

Figure 2. UML representation of the RBAC model [4]

4. USING RBAC IN THE CLOUD

Each access control model should be tailored to its application environment based on the context and scope of protection required by the environment. It is

straightforward to extend RBAC from traditional fields (for example, database systems and network applications) to cloud computing environments. To successfully employ the RBAC model, the first task is to identify corresponding entities defined in Figure 2. Due to the difference in nature and scope, it is important to separate the identification among each of the three services (SaaS, PaaS, and IaaS) in the SPI model.

4.1 Users/Groups

The RBAC display gives an approval administration to clients. In this specific situation, "clients" alludes to people or programming/equipment/organize segments inside the cloud. Under the scope of security strategies, clients of the safe distributed computing condition can be grouped by their activity capacities. In Software as a Service (SaaS), clients could incorporate individual customer, corporate purchaser, and web benefits that demand assets. Stage as a Service (PaaS) is a more current administration and hasn't been completely conveyed yet, and its security strategies are yet to find. Clients in PaaS could incorporate all clients recognized in SaaS. A PaaS client would require managerial access to determine arrangement for their application running in the cloud, yet they ought not to influence other approach areas. All things considered, Users in PaaS could be characterized in a better granularity. For instance, shoppers have the benefit to characterize their own clients in a strategy area. Foundation as a Service (IaaS) is the freshest administration gave by the cloud. In IaaS, clients may incorporate those characterized in PaaS, in spite of the fact that web administrations are more outlandish. Much of the time, an IaaS client will get access to a virtual machine and be in charge of arranging all parts of the framework. In that capacity purchasers have the most control over the meaning of clients/operators when it is contrasted with other two administrations, and the clients could be characterized at a better level.

4.2 Roles

Parts are ordered by their activity capacities. Illustrations incorporate database administrator and framework overseer. The meaning of parts is integral to the RBAC show and is exceptionally identified with application conditions. In distributed computing, parts can be characterized at an abnormal state. They may incorporate purchaser, inhabitant, and specialist organizations. Utilizing a better granularity, these parts can be additionally part in a few ways. The first is as indicated by the particular gets to, for example, program get to, information get to, Internet access, and server get to. For instance, a part might be characterized as "shopper for Internet gets to". The second route is by following the three administration models – SaaS, PaaS, and IaaS. For instance, a part might be characterized as "occupant for corporate information gets to." The third method to part is by following cloud models characterized by sellers [13]. Along this line the parts can be additionally part at better levels and the whole structure of parts at long last frame a progressive system, in which parts could acquire consents and capacities characterized in a parent part. Legacy is one particular trademark in RBAC and appears to fit well in this circumstance. For instance, at a coarse granularity level, in Amazon's Elastic Compute Cloud (EC2), parts may be characterized as EC2 example 1 manager, EC2 occasion 1 administrator, and so on. In IBM's Blue Cloud, parts could be characterized as DB2 head, DB2 database administrator, Tivoli provisioning director, Tivoli observing operator, virtual machine case 1 client, and so forth.

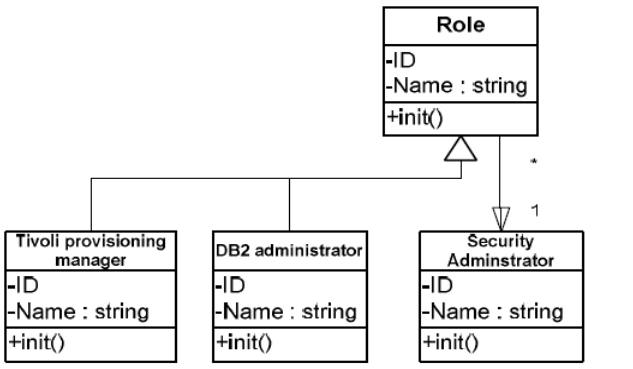

Figure 3. Example Admin roles in IBM Blue Cloud

Figure3 shows an example how the administrator roles could be organized in IBM Blue Cloud. Similar break-downs can be performed for daily operator roles. The security administrator is a single role that oversees all security functionalities in the system. It is also a composite role that inherits privileges from "Tivoli provisioning manager" and "DB2 administrator". When more roles are designed, they can be organized into hierarchies to facilitate their management. How the roles are designed and managed greatly affects the scalability of RBAC in the cloud. It can be seen that, in these given examples, the roles in the cloud platforms are relatively easy to identify because their job functions can be clearly separated, and users can be assigned accordingly. These roles are highly specific not only because of their service providers, but also be tailored to their business requirements. These are the situations in which RBAC is the one of the best fit access control model for cloud computing. In the IaaS model or a private cloud, since consumers have full control over the virtualized environment, the roles can be defined according to their specific needs. For example, for a banking system, traditional roles such as "cashier" or "accountant" could be defined. In the system there could also be roles adapted to the cloud environment, for example, a role can be named as "cloud security administrator." It is quite possible that a role with the same name may incorporate completely different access privileges in different environments.

4.3 Permissions

Permissions are defined according to job functions of roles. In a secure cloud computing environment they can generally be classified into the following groups: data access permissions, program access permissions, and service access permissions. Access permissions should be configured according to the environmental requirements. For example, program permissions include read, write, execute, create,

and delete. Service permission may include bandwidth utilization, computational power utilization, etc. Similar to the discussion presented in the previous section, the permissions can be further split in finer granularities and in hierarchies.

4.4 Protected objects

In the object-oriented domain, protected objects represent resources within the clouds. There are in general three groups of protected objects, data, program, and service. These objects correspond to permissions mentioned earlier. If permissions are defined at a finer granularity, the project objects should be identified accordingly. For example, in Amazon's EC2, objects can be defined as EC2 instance 1, EC2 instance 2, etc. There are three EC2 instances (protected domains) in this example

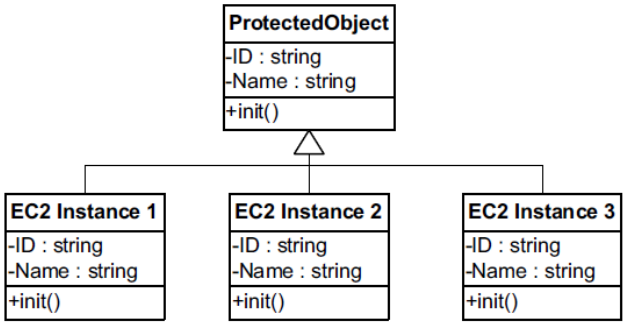

Figure 4. Sample protected objects in Amazon EC2

4.5 Sessions

Sessions are used in RBAC models to define ways to use multiple roles. The use of sessions in cloud computing is almost the same as that in traditional application environments. The process can be briefly shown in Figure 4. In the figure5, attribute ActiveRoleList provides links to current active roles for a user. Attribute RoleList provides links to all roles where the current user is a member. ActiveRoleList is a subset of RoleList. We can check whether a user is a member of a role by invoking checkUserRole(). To activate or deactivate roles where a user is a member, we can invoke roleActivation() and roleDeactivation() routines. This mechanism can be used to enforce role exclusion or inclusion at execution time. A session can be established using SessionEstablishment(). The session can be disabled using SessionRevocation(). By using sessions, one can manage dynamic role inclusion/exclusion owned by each user. Permissions can be disabled and enabled through the use of sessions. It should be noted that according to the definition by Ferraiolo et al. [14], "each session is a mapping between a user and an activated subset of roles that are assigned to the user". A session is not necessarily limited to one user or one role. In cluster-computing environments, parallel assignments of multiple sessions to one role can be easily achieved. Parallel implementations can also be done for user-to-role, object-torole, permission-to-role, permission-to-operation and permission-to-object assignments.

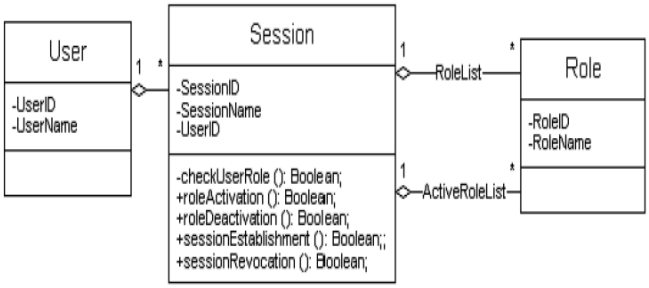

Figure 5. Relationship among User, Role and Session [12]

In addition to the identification of different entities in RBAC, there are also some management issues should be considered. One issue is who should manage the assignment of the roles. In cloud computing, there needs collaboration between cloud vendors and consumers so that a fine-grained definition on roles can be achieved. This is especially true for the SaaS and PaaS model. Another issue is how to handle dynamic role management. In RBAC, an end user may change its role from to another. The revocation of access to data and services should be carefully evaluated so that the change does not grant unauthorized access in the cloud. The change may have cascading effect when a multi-party trust chain is formed – this may require coordination of multiple cloud providers. In addition the use of RBAC should be closely administered and monitored so that policy and compliance (for example, Health Insurance Portability and Accountability Act or HIPPA – a US law that address the security and privacy of health data) could be enforced.

5. DISCUSSION

Clearly RBAC has incredible possibilities to be utilized as a part of distributed computing in different settings. However because of the absence of principles and regularly concurred accepted procedures in the field, the usage of RBAC is seller particular. It gives the idea that the SaaS is by a wide margin the most develop benefit models in distributed computing. The utilization of RBAC can be extraordinarily upgraded by the advancement of the cloud merchants, and could gather encounters when the model is extended to other administration models. Expansive corporate purchasers should put resources into outlining a good example that maps client parts to their inside business works keeping in mind the end goal to viably deal with the RBAC show. Some current encounters with RBAC could be connected amid the procedure. Shoppers of RBAC should take note of that even with an industry standard, the seller purchaser still need to concede to the names and semantics utilized inside the cloud benefit. For instance, a "security manager" could mean diverse parts in the corporate setting and in a cloud setting. An approach is requiring so corporate parts can be isolated from parts characterized by cloud suppliers [5]. It ought to likewise be noticed that RBAC may not fit into all security areas in distributed computing. Its quality seems to lie in zones in which work elements of various parts can be unmistakably characterized and isolated, and parts have an object oriented nature and could shape a pecking order. As a rule different access control model might be utilized [5]. For

instance, the MAC demonstrate is important to settle on get to control choices in light of the order of benefits or data. Web benefit access to assets in the cloud is by and large best bolstered by a DAC (i.e., Access Control List or ACL) demonstrate. In a few circumstances, cloud situations may force standard based or assignment based access control, contingent upon the administration assertion amongst buyers and cloud suppliers. There are likewise industry standard utilized in distributed computing. One case is the eXtensible Access Control Markup Language (XACML), which points "to characterize a center blueprint and relating namespace for the outflow of approval strategies in XML against objects that are themselves distinguished in XML." [15].

6. CONCLUSIONS AND FUTURE RESEARCH

This paper presents a brief discussion on cloud computing and its related security risks, with a focus on access control and RBAC. RBAC models can be used to implement three important security principles: least privilege, separation of duties, and data abstraction. Through the discussion it can be seen that RBAC has great potentials to be employed in cloud computing. However due to the lack of standard and best practices in the field, and also due to the immaturity of the cloud computing itself, huge efforts are still necessary to promote RBAC and make access control effective. Future research efforts should include a more formal identification process for different entities in RBAC in the context of cloud computing, industrial standards and best practices of using RBAC in their clouds, and large scale experiments to show the promise of RBAC. It appears that the success or RBAC will be in pace with the maturity of the cloud computing platform.

REFERENCES

1. "Gartner outlines five cloud computing trends that will affect cloud strategy through 2015," Gartner Press Release, 2012.

2. Jansen W. and Grance T. (2011). Guidelines on security and privacy in public cloud computing. NIST Special Publication 800-144.

3. W. Li, S. Li, and H. Wan, "An Access Control Mechanism in Cloud Computing Environments," Proceedings: 2011 National Annual High Performance Computing of China (HPC China 2011). October 2011, Jinan, China, China Computer Federation.

4. R. L. Krutz, and R. D. Vines. Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Wiley Publishing, Inc, 2010.

5. M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, On Technical Security Issues in Cloud Computing, 2009 IEEE International Conference on Cloud Computing, pp. 109-116.

6. R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role-Based Access Control Models," IEEE Computer, Vol. 29, No. 2, February 1996, pp. 38-47.

7. D. Ferraiolo and D.R. Kuhn, "Role Based Access Control," Proceedings of the 15th Natl. Computer Security Conference, 1992, Baltimore, MD, October 1992, pp. 554-563

8. Cloud Security Alliance. Domain 12: Guidance for Identity & Access Management V2.1, Retrieved28July2011from https://cloudsecurityalliance.org/wpcontent/uploads/2011/07/csaguide-dom12-v2.10.pdf.

9. J. Bacon, K. Moody and W. Yao, "Access Control and Trust in the Use of Widely Distributed Services," Proceedings: Middleware 2001, Heidelberg, Germany, November 2001, IEEE, pp. 300-315.

10. M. E. Shin and G. Ahn, "UML-Based Representation of Role-Based Access Control," Proceedings: IEEE 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE'00), Gaithersburg, Maryland, 2000, IEEE Computer Society, pp. 195-200.

11. E. B. Fernandez and R. Pan, "A Pattern Language for Security Models," Conference on Pattern Languages of Programs (PLoP) 2001, Retrieved 24 July 2011 from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.5898&r ep=rep1&type=pdf.

12. W. Li, E. Allen. An Access Control Model for Secure ClusterComputing Environments. Proceedings of the 38th Hawaii International Conference on System Sciences (HICSS'05). Big Island, HI, January 3-6, 2005, p. 309.

13. G. Boss, P. Malladi, D. Quan, L. Legregni, and H. Hall. Cloud computing. IBM White Paper, 2007,Retrieved24July2011from http://download.boulder.ibm.com/ibmdl/pub/software/dw/wes/hipods/Cloud_computing_wp_final_8Oct.pdf.

14. D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chadramouli, "Proposed NIST Standard for Role-Based Access Control," ACM Transactions Information and System Security, Vol. 4, No. 3, August 2001, pp. 224-274.

15. Extensible Access Control Markup Language (XACML), OASIS, Retrieved 24 July 2011 from http://xml.coverpages.org/xacml.html.

16. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing", Tech. Report

UCB/EECS-2009-28, EECS Dept., University of Califonia, Berkeley, 2009.

17. W. Li, S. Li, and H. Wan, "An Access Control Mechanism in Cloud Computing Environments," Proceedings: 2011 National Annual High Performance Computing of China (HPC China 2011). October 2011, Jinan, China, China Computer Federation.

18. Y.Chen, V.Paxson, and R.H.Katz,"What's new about Cloud Computing security", Tech. Report UCB/EECS-2010-5, EECS Dept., University of Califonia, Berkeley, 2010