www.ijecs.in
*International Journal Of Engineering And Computer Science ISSN:2319-7242*
*Volume 4 Issue 3 March 2015, Page No. 10737-10739*

# A Survey Report on Risk-aware Role-based Access Control Model

***Bhoomi Pipaliya*** [1]***, Vinay Harsora*** [2]

[1,2]*Computer Engineering, RK University*
*Rajkot*

[1]bhoomipipaliya@gmail.com

[2]vinay.rkcet@gmail.com

***Abstract*— Cloud computing is an advanced emerging technology that uses internet to provide reliable, convenient, on-demand services to customers. One of the interesting and most challenging area in cloud computing is access control model. MAC, DAC, RBAC, etc are traditional access control methods which controls the access to services and resources. Role based access control (RBAC) allows access based on role(s) assigned to a particular object, which increases security. There exist some risks like insider threats in RBAC. Risk-aware role based access control (RAAC) provides a mechanism that can manage the access to resources using two approaches of RAAC: traditional approach and quantified approach.**

***Keywords*— Access control, security, risk, RBAC, RAAC**

## I. Introduction

Cloud computing is an advanced emerging technology that uses internet to provide reliable, convenient, on-demand services to customers. In the past all the computer applications were developed and used in local systems. It created a problem in case of system crash. It destroys all those computer applications used in that local system. To overcome this problem cloud computing was introduced. It is internet based model which provides services on the internet to the customers. Cloud computing allows businesses and consumers to use applications without installation and access their personal files at any computer with internet access. Advantages of cloud computing like lower cost, high performance, freedom from up gradation and maintainance, scalability, speedy implementation, mobility, increased storage capacity, etc. made cloud computing technology widely acceptable[1]. Cloud computing is "pay-per-use" model, which makes cloud services cost effective.

National Institute of Standards and Technology [2] defines Cloud Computing as:

*"Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources(e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*

Cloud delivers IT resources to consumers as different services. These services are classified as Infrastructure as a service (IaaS), Platform as a Service (PaaS), Software as a Service (Saas).

*1) Infrastructure as a service (IaaS):* It delivers infrastructure resources as a service, such as data storage, processing power and network capacity. "The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of networking components (e.g., host firewalls)"[3].

*2) Platform as a Service (PaaS):* It delivers the services as operation and development platforms. The consumer uses the platform to develop and run his own applications, supported by cloud.

*3) Software as a Service (Saas):* The SaaS service model offers the services as applications to the consumer, using standardized interfaces. The services run on top of a cloud infrastructure, which is invisible for the consumer [3].

There are four different deployment models of cloud computing. They are Public Cloud, Private Cloud, Hybrid Cloud and Community Cloud.

*1) Public Cloud:* A public cloud or external cloud, is the most common form of cloud computing, in which services are made available to the publicly in a pay-as-you-go manner [4].

*2) Private Cloud:* A Private Cloud, or internal cloud, is used when the cloud infrastructure, proprietary network or data centre, is operated solely for a business or organization and serves customers within the business firewall [4].

*3) Hybrid Cloud:* A composition of the two types (private and public) is called a Hybrid Cloud, where a private cloud is able to maintain high services availability by scaling up their system with externally provisioned resources from a public cloud when there are rapid workload fluctuations or hardware failures [4].

*4) Community Cloud:* The idea of a Community Cloud is derived from the Grid Computing and Volunteer Computing paradigms. In a community cloud, several enterprises with similar requirement can share their infrastructures, thus increasing their scale while sharing the cost [4].

## II. ACCESS CONTROL MODEL

Cloud provides resources like software and hardware as a service to the consumers over the internet. End users access them as they need through a web. Access Control's role is to control and limit the actions or operations in the Cloud systems that are performed by a user on a set of resources [5]. Access control gives the authorization to the users to access resources that are publicly available to the users. Access control is a mechanism which manages the access of users to a set of resources. Access control increases security of a system and gives predefined access to the resource. Access control is a policy or procedure that allows, denies or restricts access to a system [6].

The various types of access control mechanisms are developed. DAC (Discretionary Access Control), MAC (Mandatory Access Control), RBAC (Role Based Access Control) are traditional access control mechanisms. Access control mechanisms are used to mediate the every attempt of particular users to the object based on the access privileges given to the system [7]. All these mechanisms are discussed below.

*A. Discretionary Access Control (DAC):*

DAC is the traditional access control mechanism in which user is given complete control over all the programs or resources. DAC allows access on the base of user identity and authorization which is defined for open policies. DAC is the mechanism which manages who can access what. In DAC owner of the resource grants the access permission to the end user. DAC mainly deals with the following that are Inheritance of permissions, User Based Authorization, Auditing of system Events and Administrative privileges [7].

Including advantages [7] such as flexibility of usage on information and maintain the authorization database, it has some limitations. There is no assurance on flow of information and there is no restriction on the usage of information which results in loss of information. It can be easily attacked and there is no consistency on information. There might be a chance that owner may change the DAC policies by inserting malicious program.

*B. Mandatory Access Control (MAC):*

MAC is mainly concerned with confidentiality of information. This model treats these threats by controlling access centrally. An ordinary user cannot change the access rights a user has with respect to the file, and once a user logs on to the system the rights he has are always assigned to all the files he created [8].MAC policy takes decision based on network configuration. Each object present in cloud environment assigned some security level, which helps to identify the current access state of the object.

MAC includes advantages [7] like, in MAC information integrity will increase and it prevents the flow from low objects to high objects. It is mainly used in military and government applications. It provides multilateral security. Disadvantage of MAC is that once the security level is identified to particular subject in the hierarchy it will not modify the security level.

*C. Role Based Access Control (RBAC):*

In RBAC access decisions are based on the individual's roles and responsibilities within the cloud environment. It restricts system access to authorized users only. Every authorized user is given a specific role(s). Permissions or access is granted based on these roles. Role is a set of objects or policies related to the subject. Role may vary from user to user. RBAC provides web based application security. It allows users to execute multiple roles at the same time. RBAC decides what permission should be assigned to which user. RBAC is used to implement DAC as well as MAC.

Advantages of RBAC includes it minimizes the damage of information by intruders. It provides classification of user based on their execution environment. Disadvantage of RBAC is permissions associated with each role can be deleted or changed.

RBAC has many advantages, few of which overcome limitations of other two traditional mechanisms. Therefore some other RBAC approaches are developed.

In addition to traditional mechanisms described above few more mechanisms are developed to make system and resources more secure. These are described below.

*D. Risk-Aware Role-Based Access Control (RAAC):*

The core goal of RAAC is to provide a mechanism that can manage the trade-off between the risks of allowing an unauthorized access with the cost of denying access when the inability to access resources may have profound consequences [9]. RAAC mainly works based on authorization decision function, which takes decision by calculating risk i.e., how much risk is generated by allowing access or denying access. RAAC calculates risk matrix each time user creates a request. Based on the value of risk matrix, it manages the access rights.

RAAC has mainly two approaches: traditional approach and quantified approach. [10] Contains framework of RAAC. Traditional approach works statically, it means constrains are designed for every user role at the time of role generation. On the other side quantified approach works dynamically, it means whenever user creates a request, risk is calculated and compared with risk threshold. Therefore, constrains are designed at every session.

The quantified risk-aware approach is categorized into two types: Non-adaptive approach and Adaptive approach. In non-adaptive approach risk-threshold is calculated dynamically each time of session generation. Based on this risk-threshold each time user request is either allowed or denied. Adaptive approach works similarly to Non-adaptive approach, except in adaptive approach continuous monitoring of user activity is performed. Here, risk-threshold value is lowered to stop user activities in case user is identified doing abnormal activities and vice verse. Continuous monitoring in adaptive approach makes it more secure but complex.

*E. Attribute Based Access Control (ABAC):*

ABAC works with identification, authentication, authorization and accountability. ABAC allows access to users based on policies which use the combination of attributes. Attributes can be any type of attributes like user attributes, resource attributes, environment resources, etc. Attributes are set of labels that can be used to identify an object (i.e. user, resource, environment, etc.). It is capable to enforce DAC as well as MAC. RBAC has a problem of assigning privileges to the user, which is solved by ABAC. It considers attributes of user request.

*F. RBAC-A:*

D. Richard Kuhn et al., [13] propose a model which combines the best features of Role Based Access Control (RBAC) with Attribute Based Access Control (ABAC) to design a simple and flexible model [12]. RBAC does not support dynamically changing domain and ABAC is flexible but lack of RBAC's clarity, so they are merged and new model is called RBAC-A.

It is simple and flexible. It is more flexible than RBAC because it does not require separate roles for relevant sets of subject attributes. RBAC-A uses three approaches to handle the relationship between roles and attributes namely: Dynamic roles, Attribute-centric and Roles-centric.

### *G. distributed RBAC (dRBAC):*

dRBAC supports large distributed system. Therefore it is used in multiple organizations. It solves the problem of giving access control in multiple organizations. dRBAC has the following problems: This dRBAC method has the higher time complexity and high space complexity. Due to the increasing nature of cloud users and sequential access of resources which will cause the redundancy and inconsistency of information access and this will cause the complex cross domain problems [7].

### *H. Cloud optimized RBAC (coRBAC):*

coRBAC inherits the functionality of both dRBAC and RBAC [11]. So it improves the certification process. The major drawback of conventional RBAC is excess time of authentication and login time. But coRBAC improves the overall efficiency [7]. CoRBAC reduces the following [11]:

i) Unnecessary process of establishing secure connection

ii) There is no need of setting up multilevel cache

iii) Space and time complexity of access control system is reduced.

## III. Conclusion

This paper gives brief introduction about cloud computing and access control model also brief discussion about RAAC. Cloud computing is widely accepted and challenging area. Now-a-days, when businesses and organizations are moving toward cloud, there is a quite necessity of security. Access control model increases security by allowing access to authorized users only and by denying access to unauthorized users. Many mechanisms are developed in access control models as briefly explained in this paper.

## References

[1] Rajnish Choubey, Rajshree Dubey, Joy bhattacharjee, “A Survey on Cloud Computing Security, Challenges and Threats”, International journal on Computer Science and Engineering, Vol. 3 No. 3, March 2011

[2] P.Mell, “The NIST Definition of Cloud Computing”, U.S. Department of Commerce: Special Publication 800-145.

[3] Subedri Mithila, P. Pradeep Kumar, “Data Security through Confidentiality in Cloud Computing Environment”, International Journal of Computer Science and Information Technologies, Vol. 2 (5), 2011

[4] R. Martin “IBM brings cloud computing to earth with massive new data centers”, Information week Aug. 2008

[5] Mavridis Ioannis “Towards new access control models for cloud computing systems”

[6] Yingjie Xia, Li Kuang and Mingzhe Zhu “A Hierarchical Access Control Schemes in Cloud using HHECC” Information Technology Journal 9 (8): 1598-1606, 2010

[7] Punithasurya K, Jeba Priya S “Analysis of Different Access Control Mechanism in Cloud”, International journal of Applied Information Systems, Vol. 4, September 2012

[8] Parmindar Singh, Sarpreet Singh “Cross Bread Role based Acces Control for Exteded Security at Azure in Cloud Computing” Internatonal Journal of Application or Innovation in Engineering and Management, Vol, 2, February 2013

[9] Liang Chen, Jason Crampton “Risk Aware Role Based Access Control”, 7th International workshop, STM 2011, June 2011

[10] Khalid Zaman Bijon, Ram Krishnan, Ravi Sandhu “A Framework for Risk-Aware Role Based Access Control”, 6th Symposium on Security Analytics and Automation 2013

[11] Zhu Tiayni, Liu Weidong, Song jiaxing “An Efficient role based access control system for cloud computing”, 2011 11th IEEE International Conference on Computer and Information Technology.

[12] R. GnanaJeyaraman, Dr. D. Gunaseelan, P.K. Kumaresan “Information Assurance through Access Control Policies: A Comprehensive Study”, International Journal of Computer & Organization Trends, Vol 6 Number 1, March 2014

[13] Richard Kuhn, Edward J Coyne, Timothy R. Weil “Adding Attributes to Role-Based Access Control”, Computer, Vol 43 Number 6, pp. 79-81, June 2010, doi:10.1109/MC.2010.155