TRJ VOL. 2 ISSUE 4 JULY-AUG 2016 ISSN: 2454-7301 (PRINT) | ISSN: 2454-4930 (ONLINE)
DOI: 10.13140/RG.2.1.3381.1443

Review on advanced access control models in cloud computing

Iqbalinder Singh Sohal[1], Amardeep Kaur[2]
Student (M.Tech), Assistant Professor
Punjabi University Regional Centre for Information Technology and Management, Mohali

Abstract- Security level is one of the most impactful aspects of a technology in wide spreading it and making it popular in the industry. Access control has a similar effect in the success of cloud computing. It helps to build a higher trust level on the service provider and hence provide better Quality of service. In this review paper, we present the study over traditional and advanced access control models. Access control models are explained with the help of simplified model diagrams, which will help the researchers to build a faster and better understanding of the access control models. We have also listed the advantages and disadvantages of the access control models, which could help to select an access control model according to the need and type of the access required to set up the cloud environment.

Keywords- *Security Level, quality of services, cloud environment and access control model.*

1. INTRODUCTION

The emerging internet technology i.e. Cloud computing is the one which grants on-demand **access** to a shared, networked and distributed pool of resources without requiring any kind of extensive management efforts on behalf of the clients that require these resources. It's easy to differentiate cloud computing from other classical computing models by five major characteristics such as broad network access, rapid elasticity, resource pooling, measured services and on-demand self-service [5]. Access Control is one of the basic and fundamental security components in cloud computing and for the most part it is an approach or security technique that permits denies or limits access to a system/system resource. It permits one application to believe the identity of another application [1] [2] [6]. It limits what a client of a cloud provider can do directly, preventing the act of breaching security. Access control includes addressing issues of authorization, authentication and administration.

The customary model for access control is application-driven access control, where every application monitors its accumulation of clients and manages them, is not plausible in cloud based designs. Since this technique requires a ton of memory for putting away the client subtle elements, for example, username and password. So cloud requires a client driven access control where each client request to any cloud service provider is packaged with the client character/identity and entitlement data [3].

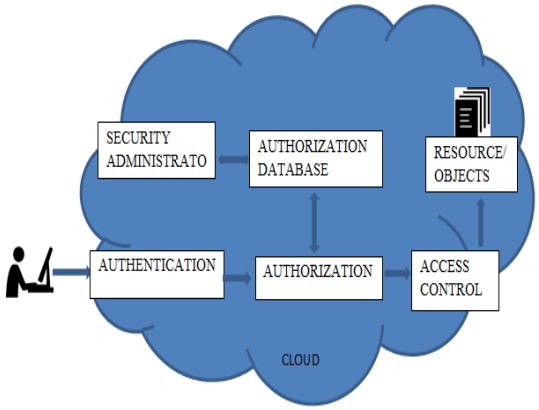


Fig.1.Security services of access control

Access control models can be generally arranged into following three classifications:

(1) Discretionary access control (DAC): Owner of the object restricts the access privilege for other users based on their identity. In simple words, owner of object is the boss of access control over the object
(2) Mandatory access control (MAC): Administrator of the system restricts the access privileges for all the users.
(3) Role-based access control (RBAC): A user can have access over the object based on his/her role in the system

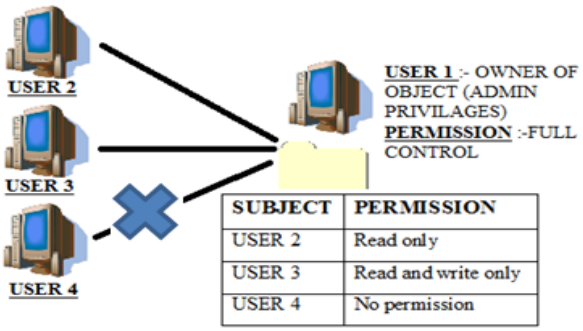
Above described DAC and MAC are identity based access control models, users and objects (resources) are distinguished by unique names and cannot be used in cloud computing environment, where various nodes may not know each other [1][7]. Identification could be done straightforwardly or through assigned roles. In today's rapidly developing application oriented cloud environment, access control models should be developed according to the need or desire of the system.

In this paper, I present a review of existing access control models with which are developed according to the desire and need of the company. The remainder of the paper is organized as following ----

DOI: 10.13140/RG.2.1.3381.1443

A. Various access control methods in cloud computing

1) *Discretionary access control (DAC):* - This is the conventional access control in which client has the complete control over the project. DAC is based on offering access to the client on the premise of client character and approval which is characterized for open policies. DAC policy depends on the client's identity and authorization that indicates for every client's access strategy and object that is requested by client. DAC has access attributes and access rules, the access attributes permits the system to define various authorization levels, and the access rules prevent the unauthorized clients to access any information [8][9].



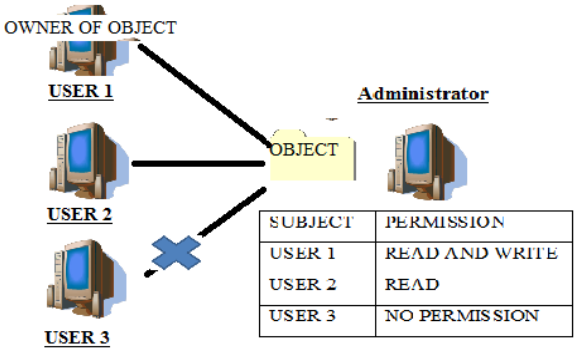
SUBJECT	PERMISSION
USER 2	Read only
USER 3	Read and write only
USER 4	No permission

Fig.2.Model diagram of DAC

Advantage: Adaptability in utilization by keeping up the authorization database which comprises of authorized clients.

Disadvantage: This model provides neither high level security nor risk awareness. DAC is highly prone to attacks like Trojan horse virus attack. The worst part is that it is not compatible for cloud computing implementation.

2) *Mandatory access control (MAC):* - Mandatory access control upholds the control on the basis of directions by administrator. The most common form of mandatory access control is the multilevel security access control, based on subjects and objects in the system. Objects acts as passive entities and store data while Subjects acts as active entities and sends access request to the objects [8][9]. A central administrator assigns a security level on data based on its significance and sensitivity. It additionally assigns a security clearance to users. Only the users with security clearance level more prominent than the security level of the data can have access to the data.



SUBJECT	PERMISSION
USER 1	READ AND WRITE
USER 2	READ
USER 3	NO PERMISSION

Fig.3.Model diagram of MAC

Advantages: -As only system administrator can access or change the control, MAC provides strong security and also it reduces security errors.

Disadvantages: - It doesn't promise complete protection of data. The system administrator is vulnerable to attacks since it is the one who knows about the security levels. Additionally this model is costly to implement [10].

3) *Role based access control (RBAC):* - Role based access control upholds the control on the basis of role assigned to the user. User's role determines his security clearance. RBAC model can be utilized to execute a few essential security standards, for example, least privilege, separation of duties, and data abstraction. RBAC has various administrative policies such as centralized, hierarchical, co-operative, ownership and decentralized [8] [9] [11][26].

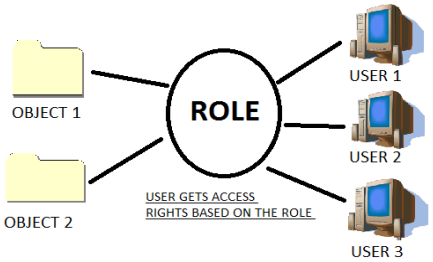


Fig.4.Model diagram of RBAC

Advantages: - As roles are assigned on the minimum privilege access, it decreases the level of damage. Separation of roles limits the chance of misuse of data.

Disadvantages: - Users with multiple roles could use one role to grant access to an object which is restricted for his other role. This is a violation of security policy.

DOI: 10.13140/RG.2.1.3381.1443

4) *Attribute based access control (ABAC):* - In an open and decentralized cloud environment where the client population is ever-changing and identity of all clients is not recognized, roles assignment modeling becomes inappropriate. To address this scenario and make access decisions, ABAC model was proposed which is based on the user attributes and are considered on the bases of user's request. ABAC usually considers identification, authentication, authorization and accountability which make it more secure, saleable and flexible [8][12].

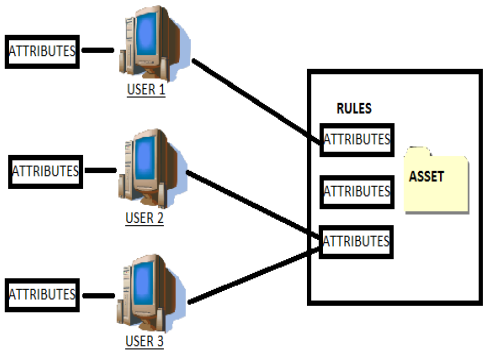


Fig.5.Model diagram of ABAC

Advantages: - ABAC solves the problem of assigning privileges to the clients as it is based on the set of attribute.

Disadvantages: - Until now, this model has not been implemented in recognized applications because of its difficult to implement a suitable security policy for a huge diversity of users [10].

5) *Risk aware access control (RAAC):* - The standard RBAC model is intended to work in a generally closed and stable environment and does include any provision for risky situations. It is based on the constraint specifications and verifications (Risk-engine). The objective of RAAC model is to deal with the trade-off between the risks of permitting unauthorized access with the expense of denying access when the helplessness to get to resources may have significant outcomes. This methodology is especially helpful to allow some risky access in a crisis circumstance [13] [14] [15].

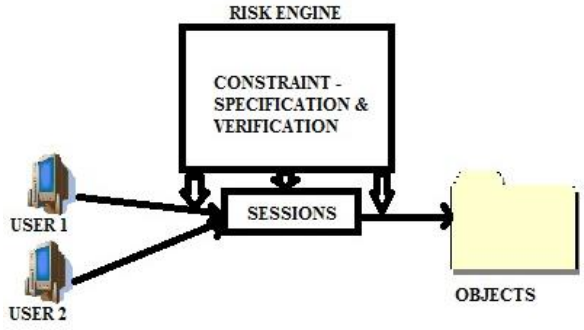
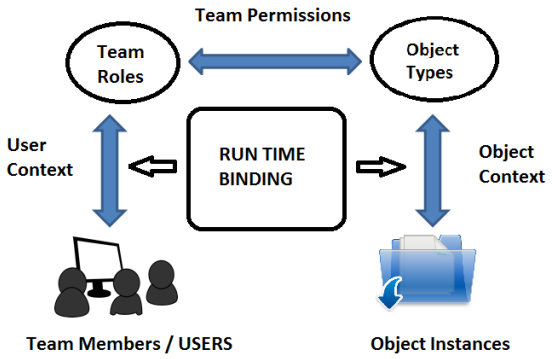


Fig.6.Model diagram of RAAC

Advantages: - As risk is represented as a metric, it can be regarded as a quantified approach. The most important advantage of RAAC is that under every situation there is a calculated value of risk.

Disadvantages: - Firstly this model is very hard to implement as the logic to define the risk level needs a lot of analysis and planning. Proper training is required for the administrators to cope with RAAC model.

6) *Team based access control (TMAC):* -TMAC approach was introduced to address the team oriented access control in cooperative environment. TMAC is an extended approach of RBAC for multiple organization collaboration to perform a task. The basic idea behind TMAC includes the use of RBAC to outline a set of permissions on roles and objects. A unique team will include unique set of team roles thus inheriting unique set of team permissions. Teams having same structure will include same set of team roles thus inheriting same set of team permissions. Also, TMAC requests for the run time binding of the team permissions for each team to the sets of team users and object instances of the team. This activates the user level permissions at the run-time [12] [16].



DOI: 10.13140/RG.2.1.3381.1443

Fig.7.Model diagram of TBAC

Advantages: - TMAC has the benefit of having the capacity to offer the administrative and modeling aspects of RBAC and yet providing the individual users and objects, a fine-grained control over permission activation [16].

7) *Trust based access control:* - Cloud computing have the challenges of dynamic, elastic, highly scalable systems. To address these challenges, multiple levels of trust are integrated into access control model. In TBAC, user gets access privileges based on his trust level, which in turn depends on related information [23] [24].

Advantages: - The major advantage of TBAC model is that it allows operational needs to dominate security risk.

Disadvantages: - TBAC model has been generally proposed as an extension of RBAC and in RBAC model, the clients are assigned roles according to the job requirements and responsibilities, not trust levels. TBAC model fails to bag the key semantics of RBAC systems [25].

8) *Location based access control:* - In this model, access rights are granted after checking the location of user/client. LBAC model supports role hierarchy but doesn't support SoD (separation of duties). Various extended LBAC models are proposed in accordance to the need such as LRBAC: Location aware role based access control model [17], Geo Social RBAC: a location-based socially aware access control framework [18], LMAC: location-based mandatory access control model [19], TLRBAC: Time and Location Based Services with Access Control [20],

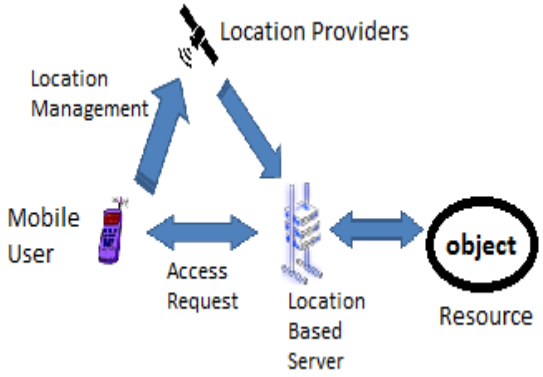


Fig.8.Model diagram of LBAC

Advantages: - It provides greater flexibility as well as security to the cloud computing architecture.

Disadvantages: - Protection from the malicious attacks on the platform.

9) *Temporal role based access control:* - This can be regarded as an extension to RBAC, with an additional time dimension to the RBAC model. This model presents the concept of role enabling and role disabling based on the temporal constraints. Access can be granted only to an activated role i.e. a role which has been enabled will get access to the requested objects [20] [21]. Another extension based on the time oriented RBAC was proposed in X-GTRBAC: an XML-based policy specification framework and architecture for enterprise-wide access control [22] [27].

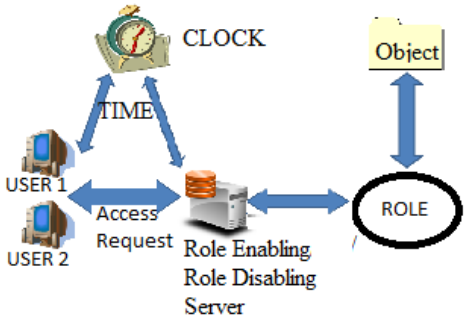


Fig.9.Model diagram of TRBAC

Advantages: - A client having a certain role will get access privilege, only in the hours permitted by their clock cycle which is administrated by administrator. This makes it a very secure access control model. Intruders from other than permitted time cycle will never be able to get authentication over any object.

Disadvantages: - A client with multiple roles and cyclic shifts might be hazardous at times.

10) *Context aware access control:* - The concept of context is obtained after integrating location, temporal state and trust level of the cloud platform to protect the system from the attacks of malicious insiders. It dynamically enables the permission to the clients after correlating the role of client with the context.

Advantages: - The permissions to a specific role are associated with the context based on dynamic constraints. The concept of least privilege is adopted by using role permission activation rule thus it improves the reliability.

DOI: 10.13140/RG.2.1.3381.1443

Disadvantages: - The reliability of the trust level of the platform is lost with any kind of discontinuity in the integrity.

II. CONCLUSION

The strength of any computing model lies in the various aspects of security of that technology. As cloud computing is an emerging technology, access control offers a strong security of data and is considered as a major research area. A good access control model assures a secure cloud environment. We studied several access control models and tried to explain them in a simplest way with the help of model diagrams, so that the researchers can learn and understand these access control models in an easier way.

In this paper, we studied several access control models such as DAC, MAC, RBAC, ABAC, RAAC, TMAC, TBAC, LBAC, TRBAC and CAAC. All the access control models have different mechanisms and can be employed in the various suitable cloud environments based on the advantages and disadvantages. This paper is targeted to provide an easy and better understanding of the access control models in cloud computing.

III. REFERENCES

[1]. Khan, A. R. ,"Access control in cloud computing environment." *ARPN Journal of Engineering and Applied Sciences*, *7*(5), 613-615, 2012.

[2]. B.Sosinsky, "Cloud Computing Bible," *Ed. United States of America:* Wiley, 2011.

[3]. Y.G.Min, Y.H.Bang, "Cloud Computing Security Issues and Access Control Solutions", *Journel of Security Engineering*, vol.2, 2012.

[4]. Ullah, S., Xuefeng, Z., & Feng, Z. (2013). TCloud: a dynamic framework and policies for access control across multiple domains in cloud computing. *arXiv preprint arXiv:1305.2865*.

[5]. Mell, P., Grance, T.: nist.gov, NIST special publication 800-145: the NIST definition of cloud computing. http://goo.gl/eBGBk (2011)

[6]. Onankunju, Bibin K. "Access Control in Cloud Computing." *International Journal of Scientific and Research Publications* 3.9 (2013): 1.

[7]. Meghanathan, Natarajan. "Review of access control models for cloud computing." *Computer Science & Information Science* 3.1 (2013): 77-85.

[8]. Punithasurya, K., S. Jeba Priya. "Analysis of Different Access Control Mechanism in Cloud." *International Journal of Applied Information Systems (IJAIS), Foundation of Computer Science FCS* 4, no. 2 (2012).

[9]. Samarati, Pierangela, and Sabrina De Capitani Di Vimercati. "Access control: Policies, models, and mechanisms." *Lecture notes in computer science* (2001): 137-196.

[10]. Ajgaonkar, Salil, Harish Indalkar, and Jaya Jeswani. "Activity Based Access Control Model for Cloud Computing." (2015).

[11]. Ferraiolo, David F., and D. Richard Kuhn. "Role-based access controls." *arXiv preprint arXiv:0903.2171* (2009).

[12]. Ray, Indrajit, and Indrakshi Ray. "Trust-based access control for secure cloud computing." In *High Performance Cloud Auditing and Applications*, pp. 189-213. Springer New York, 2014.

[13]. Aluvalu, RajaniKanth, and Lakshmi Muddana. "A Survey on Access Control Models in Cloud Computing." In *Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India (CSI) Volume 1*, pp. 653-664. Springer International Publishing, 2015.

[14]. Bijon, Khalid Zaman, Ram Krishnan, and Ravi Sandhu. "Risk-aware RBAC sessions." In *Information Systems Security*, pp. 59-74. Springer Berlin Heidelberg, 2012.

[15]. Chen, Liang, and Jason Crampton. "Risk-aware role-based access control." In *Security and Trust Management*, pp. 140-156. Springer Berlin Heidelberg, 2011.

[16]. Thomas, Roshan K. "Team-based access control (TMAC): a primitive for applying role-based access controls in collaborative environments." In *Proceedings of the second ACM workshop on Role-based access control*, pp. 13-19. ACM, 1997.

[17]. Ray, Indrakshi, Mahendra Kumar, and Lijun Yu. "LRBAC: a location-aware role-based access control model." In *Information Systems Security*, pp. 147-161. Springer Berlin Heidelberg, 2006.

[18]. Baracaldo, Nathalie, Balaji Palanisamy, and James Joshi. "Geo-Social-RBAC: A Location-Based Socially Aware Access Control Framework." In *Network and System Security*, pp. 501-509. Springer International Publishing, 2014.

[19]. Ray, Indrakshi, and Mahendra Kumar. "Towards a location-based mandatory access control model." *Computers & Security* 25, no. 1 (2006): 36-44.

[20]. Bertolissi, Clara, and Maribel Fernánde. "Time and location based services with access control." In *New Technologies, Mobility and Security, 2008. NTMS'08.*, pp. 1-6. IEEE, 2008.

[21]. Bertino, Elisa, Piero Andrea Bonatti, and Elena Ferrari. "TRBAC: A temporal role-based access control model." *ACM Transactions on Information and System Security (TISSEC)* 4, no. 3 (2001): 191-233.

[22]. Bhatti, Rafae, Arif Ghafoor, Elisa Bertino, and James BD Joshi. "X-GTRBAC: an XML-based policy specification framework and architecture for enterprise-wide access control." *ACM Transactions on Information and System Security (TISSEC)* 8, no. 2 (2005): 187-227.

[23]. Ya-Jun, G., Fan, H., Qing-Guo, Z., Rong, L. "An access control model for ubiquitous computing application." In the Proceedings of the 2nd International Conference on Mobile Technology, Applications and Systems, Guangzhou, pp. 1–6 (2005)

[24]. Bhatti,R.,Bertino,E.,Ghafoor, A."Atrust-based context-aware accesscontrol modelforWebservices." Distrib. Parallel Databases 18(1), 83–105 (2005).

[25]. Chakraborty, S., Ray, I. "TrustBAC: integrating trust relationships into the RBAC model for access control in open systems." In the Proceedings of the 11th ACM Symposium on Access Control Models and Technologies, SACMAT'06, Lake Tahoe, pp. 49–58. ACM, New York (2006)

DOI: 10.13140/RG.2.1.3381.1443

[26]. Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E."Role-based access control models." IEEE Comput. 29(2), 38–47 (1996).

[27]. Joshi, J.B.D., Bertino, E., Latif, U., Ghafoor, A. "A generalized temporal role-based access control model." IEEE Trans. Knowl. Data Eng. 17(1), 4–23 (2005).