International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2015): 6.391

Analysis of Common Access Control Models and Their Limitations in Cloud Computing Environment

Mojtaba Mohamamdi[1], Keshav Kishore[2]

[1]Research Scholar, AP Goyal Shimla University, School of Science and Technology, Mehli-Shoghi Bypass Road, Shimla, Himachal Pradesh, India

[2] Associate Professor, AP Goyal Shimla University, School of Science and Technology, Mehli-Shoghi Bypass Road, Shimla, Himachal Pradesh, India

Abstract: ***When it comes to relying on cloud computing, security and privacy has always been a serious concern. Replacing cloud computing with traditional means of computing is a huge risk especially for enterprises which value security the most. Due to the resource sharing nature of cloud and diverse groups of users, restricting access to resources appears to be the only way to protect information against unauthorized access. Allowing activities of legitimate users, requires a selective restriction of access to resources which can be enforced through an appropriate access control mechanism. In this paper, we will compare different access control models that are used in cloud computing namely Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role Based Access Control (RBAC) and Attribute Based Access Control (ABAC) and discuss the limitations of each model.***

Keywords: Cloud Computing, Security, Access Control Models, DAC, MAC, RBAC, ABAC

1. Introduction

One of the major reasons why enterprises are moving towards cloud computing is the fact that it enables access to the services and resources regardless of your geographical location. If an employee is far away from his office, he could still be able to access their files and catch up with their work. This however, leaves cloud computing potentially vulnerable. If an employee cloud remotely access their files from any location using internet, so could a hacker. Hence, using access control is quite necessary to make sure that only the right people have access to the right resources. Access control can be enforced by denying access unauthorized users or a group of users and setting well-defined limits on the access that is provided to the authorized users. There are a variety of access control models designed to serve this purpose. This paper will analyze some of the most common access control models used today. One of these models is known as Discretionary Access Control (DAC) which grants or restrict objects (resources) to the subjects (users). In this model the object's access policies are determined by the object's owner. A well-known example of this model can be seen in UNIX file mode which defines the read, write and execution permissions for the users. Another access control model that will be discussed is Mandatory Access Control (MAC). This model is generally more secure than DAC and that is because it assigns sensitivity labels on both the information and the users and ensures that the users have access only to that data for which they have a clearance. Role-based Access Control (R-BAC) on the other hand, has become the predominant model for advanced access control. Unlike the other two models, R-BAC grants access permissions based on the role of the users within the organization which leads to a much less complication regarding user assignments. R-BAC seems to fulfill the need of many organizations and enterprises. Last but not least, this paper will discuss another access control model called Attribute Based Access Control (ABAC). This model offers a highly flexible method by determining access policies based on the attributes of the entities (subject and object). More details will be provided on each of these models including their limitations in this paper.

2. Access Control Models

2.1 Discretionary Access Control (DAC)

Discretionary access control or DAC provides the resource access for the users in diverse access level according to the user's identity [1]. In DAC the users can give authority to other users to access certain resources but assigning and giving privileges is only done by the administrative policy. Overriding the policies is also done by the policy administrator and the users are not allowed to define the usage of resources [2]. Based on the user's identity and authorization, a set of permissions are granted to the user who has requested a particular resource [3]. Each resource or object is connected with either an Access Control List (ACL) or Access Control Matrices (ACM). An ACL consist of a list of users or groups along with a set of objects to which the users have different levels of access [4]. Access control matrices on the other hand, characterizes the rights of each subject with respect to every object in the system. Figure 1 shows a simple example of access control matrices.

	File1	File2	File3	Program1
User1	own-read-write	read-write		execute
User2	read		read-write	
User3			read	execute-read

Figure 1: Example of ACM

DAC is not normally used for environments which do not require a high level of security due to the fact that it is less secure that the other access control models [5]. DAC is

mostly used in commercial operating systems namely UNIX and Windows base platforms [6].

2.1.1 Disadvantages of DAC

Global Policy:
One of the problems with DAC is its inability of ensuring consistency and that is because the access control policies that the users decide on their resources are global policies.

Malicious Software/Programs
DAC is unable to detect malicious software or programs such as Trojan Houses which might lead to exploitation of user's authorization.

Information Flow
Due to the huge exchange of information in cloud environment, there might be multiple copies of a particular data in different objects. This makes the data available to the users who are not authorized to access the original copy.

2.2 Mandatory Access Control (MAC)

In Mandatory Access Control (MAC) [7] the access to the objects or resources is determined based on security levels. These security levels are set up and managed by the system administrator and based on the sensitivity of the information in the object [8]. The users and the objects are assigned to one of the security levels and when a user attempts to access a certain object, the system checks whether the security level of the user and the object matches or not. If it does, it allows the access and if it does not it will deny the access.

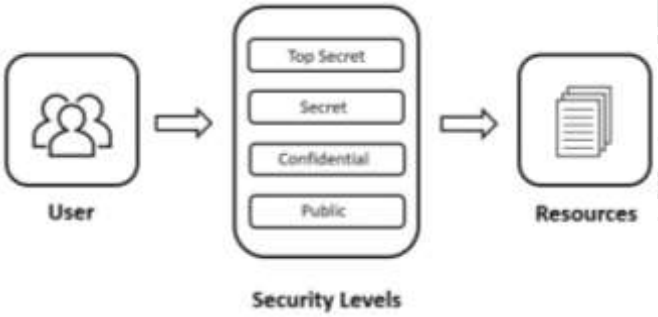

Figure 2: Example of MAC

MAC in comparison to DAC, provides a more secure model for any commercial organizations in which security is more valued than integrity. A multi-level security model, proposed by Bell and LaPadula (1973), makes DAC resilient to Trojan horse attacks [9]. This multi-level security model offered by [10] enforces a secure access control by holding two properties, no-read-up and no-write-down [11]. Using these properties, the resources will remain confidential as they restrict users to access certain objects. DAC is mostly practiced by military and intelligence agencies and not by organizations in which a dynamic changes of policy is demanded.

2.2.1 Disadvantages of MAC

Dynamic Alteration
Security policies in MAC does not support dynamic alteration due to the restrictions on the user access.

System Management
MAC requires a high system management as it needs preset planning in order to effectively implement it.

Information secrecy
Although MAC uses a multi-level security layer, it does not guarantee complete secrecy of the information. An unclassified subject for instance can write into confidential, secret or top secret objects and may possibly lead to improper modification of objects.

2.3 Role Based Access Control (R-BAC)

In Role Based Access Control (R-BAC) [12] [13] the access permissions are associated with the role of the users and each user is assigned to a set of different permissions. The roles assigned to the users can be easily reassigned [14]. Roles can also grant new permissions or can be revoked from permissions as per need of organizations. The role of the user acts as a layer that links the user with a set of permissions.

Figure 3: Example of R-BAC

The main difference between R-BAC and the other two models (DAC, MAC) is that R-BAC grants permissions to a group of users who share the same role rather than to each individual user. This makes R-BAC greatly simple when it comes to managing permissions [14]. Another main feature of R-BAC is its hierarchical structure of roles within an organization meaning a role can inherit permissions from other roles [15]. Fig. 4. Shows an example of role hierarchy in R-BAC.

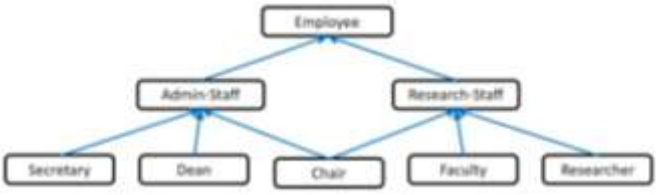

Figure 4: Example of Role Hierarchy

2.3.1 Disadvantages of R-BAC

Role Explosion
Increasing the number of users in R-BAC results in requiring various dimensions associated with the rules such as environmental constraints. For example if an employee can book a meeting room then we can set a permission as 'Book Meeting Room' and assign it to the role of employee but since there is no time or location defined we therefore need to create additional roles to fulfill this rule. In this case, the number of roles may exceed the number of users which makes it difficult to manage.

Dynamic Environment
R-BAC is not suited for dynamic environments because the roles are statically assigned to the users. Therefore it is difficult to change the access rights of the user without changing the role of that user [16] [17].

Fine Grained Results
While modern requirements are increasingly fine grained, RBAC remains somewhat coarse grained [18]

2.4 Attribute Based Access Control (ABAC)

As the name suggests, Attribute Based Access Control (ABAC) set permissions based the identity [19]. In ABAC access decisions are made according to the attributes of the user, attributes of the resources and the environmental conditions [19] [20] [21].

User Attributes: attributes of the subject of the system which may include name, age, office number, role, job title, security clearance, home address, date hired, etc.

Object Attributes: attributes of the resources of the system such as author, date created, size, last modified, file type, security level and so on.

Environmental Attributes: Attributes associated with the current state of the system's environment. For example, time, date, number of users logged in, free space, CPU usage, and so on.

Unlike the traditional access control models where the mutual assignment of roles, ownership or security labels were constructed by the system administrator [21], the access policies in ABAC are created based upon attributes in the system. ABAC is considered a dynamic model and is better suited for cloud environment since the access to resources is performed during the runtime. ABAC also removes the need for manual intervention when authorizing users for certain roles or security levels which leads to less complex administration in case of a large number of users. The functionality of ABAC model is shown in figure 5.

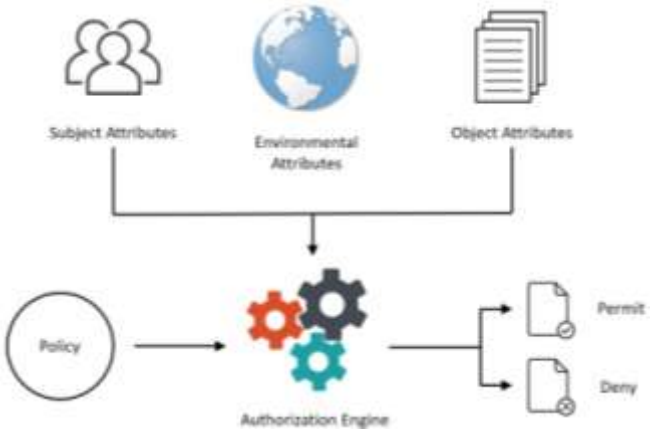

Figure 5: Example of Role Hierarchy

In spite of all the flexibilities, yet there is no standard foundational model for ABAC. There exist a large number of ABAC models, most of which however, have been domain specific and limited to a particular use case (e.g., web services) [21].

2.4.1 Disadvantages of ABAC

Hierarchical ABAC
Unlike RBAC, most ABAC models do not support the role hierarchy. This gives ABAC a less simplistic administration, both in terms of role engineering and reviewability of existing role-based policies.

Separation of Duties
Separation of duties (SoD) or segregation of duties is the notation of requiring more than one person to complete a task in order to prevent error and fraud within an organization. In R-BAC, SOD is applied through static SoD where users are not permitted to be assigned conflicting roles and through dynamic SoD, where users are not permitted to activate conflicting roles in the system. ABAC, however, lacks this key feature.

Low Expressiveness
Using ABAC model, if multiple organizations agree on a common set of standardized attributes, this would raise the problem of low expressiveness for representing the subjects and objects, therefore it losing the advantages of the flexible and dynamic ABAC functionality [22].

3. Discussion

Table 1: Comparison of access control models

Access Control Models	Advantages	Disadvantages
DAC	• Data integrity	• Does not support dynamic alteration • Requires a high system management
MAC	• Flexibility	• Global policy • Malicious software/programs • Information flow
RBAC	• Authorization management • Hierarchical roles • Separation of duties • Least privileges	• Role explosion • Not preferred in dynamic environment • Not possible to change access rights without changing the roles
ABAC	• Supports dynamic environments	• Hierarchical ABAC • Separation of Duties • Low Expressiveness

A brief comparison of different access control models has been illustrated in table 1.

4. Conclusion and Future Work

In this paper, different models of access control namely Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role Based Access Control (R-BAC) and Attribute Based Access Control (ABAC) along with their limitations with respect to cloud computing environment were analyzed. We discussed that ABAC could be replaced by the traditional access control models, however, there exist

a number of areas which could require further research in order to standardize this model to provide a more efficient and accurate management.

References

[1] Bensch, Stefan."Cloud networks for sustainable ubiquitous services."International Journal of Computational Science and Engineering 10.4 (2015): 336-346.
[2] D. Bokefode Jayant, A. Ubale Swapnaja, S. Apte Sulabha, "Analysis of DAC MAC RBAC Access Control based Models for Security" International Journal of Computer Applications, Vol. 104, Issue 5, 2014.
[3] B. Sankaraiah, D. Bhadru, G Shravan Kumar, "A Review on Different Access Control Mechanism in Cloud Environment", SSRG International Journal of Computer Science and Engineering, 2017.
[4] Azlinda Abdul Aziz, Salyani Osman, "Review the Types of Access Control Models for Cloud Computing Environment", pp. 1-5, 2015.
[5] Younis, Younis A. Kifayat, Kashif Merabti, Madjid, "An access control model for cloud computing", Journal of Information Security and Applications, Vol. 19, Issue 1, pp. 45-60, 2014.
[6] Harris S. Mike Meyers' CISSP(R) Certification Passport. 1st ed. United States: McGraw-Hill; 2002. p. 422.
[7] L. Popa, M. Yu, S. Y. Ko, S. Ratnasamy, I. Stoica, "Cloud Policy: taking access control out of the network", Proc. Ninth ACM SIGCOMM Work. Hot Top. Networks, no. 1, pp. 1-6 , 2010.
[8] A. Majumder, S. Namasudra, S. Nath, "Taxonomy and Classification of Access Control Models for Cloud Environments", pp. 23-33, 2014.
[9] Sudha Senthilkumar, Madhu Viswanatham, "Survey on Data Access Control Techniques in Cloud Computing", International Journal of Pharmacy & Technology, Vol. 8, Issue 3, pp. 17442-17461, 2016.
[10] K. Biba. Integrity considerations for secure computer systems. Technical Report MTR-3153, April 1977.
[11] D.E. Bell and L.J. LaPadula. Secure computer system: Unified exposition and multics interpretation.Technical Report ESD-TR-278, vol. 4, The Mitre Corp., Bedford, MA, 1973.
[12] Balamurugan B, Gnana Shivitha N, Monisha V, Saranya V, "Survey of Access Control Models for Cloud based Real-time Applications", International Conference on Innovation Information in Computing Technologies, 2015.
[13] Varsha D. Mali, Pramod Patil, "Authentication and Access Control for Cloud Computing Using RBDAC Mechanism", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 11, 2016.
[14] Jyoti Joshi, "Extended JV-RBAC Model with Secure API Access Control in Cloud", International Journal of Emerging Research in Management &Technology, Vol. 4, Issue 6, 2015.
[15] Priyanka Jairath, Rajneesh Talwar, "Analysis of Access Control Techniques: R3 and RBAC", International Journal of Engineering Research and General Science, Vol. 2, Issue 6, 2014.
[16] R. Sandhu. The next generation of access control models: Do we need them and what should they be? In SACMAT'01, page 53. SACMAT, May 2001.
[17] D. Ferraiolo and R. Kuhn. Role-based access controls. In Proc. of the 15th NIST-NCSC Naional Computer Security Conference, pages 554–563, Baltimore, MD, October 1992.
[18] Bernard Stepien, Stan Matwin, Amy Felty, "Advantages of a Non-Technical XACML Notation in Role-Based Models", 2011 Ninth Annual International Conference on Privacy, Security and Trust.
[19] Vijayaraghavan Varadharajan, Alon Amid, Sudhanshu Rai, "Policy Based Role Centric Attribute Based Access Control Model", Conference on Computing and Network Communications, IEEE, pp. 427-432, 2015.
[20] Khaled Riad, Zhu Yan, "EAR-ABAC: An Extended AR-ABAC Access Control Model for SDN-Integrated Cloud Computing", International Journal of Computer Applications, Vol. 132 - No.14, 2015.
[21] Daniel Servos, Sylvia Osborn, "Current Research and Open Problems in Attribute-Based Access Control", ACM Computing Surveys, Vol. 49, No. 4, 2017.
[22] Torsten Priebe, Wolfgang Dobmeier, Christian Schläger, Nora Kamprath, "Supporting Attribute-based Access Control in Authorization and Authentication Infrastructures with Ontologies", First International Conference on Availability, Reliability and Security (ARES 2006), Vienna, Austria, April 2006.

Author Profile

Mojtaba Mohammadi is a post graduate student (M.Tech) in computer science and engineering at AP Goyal Shimla University, where his area of research revolves around information security as well as cloud computing. He graduated from American University of Afghanistan (AUAF), with a bachelor degree in computer science and information technology in 2014. His interest areas are information security, cloud computing and access control mechanism for clouds. Currently he is doing research on cloud computing security.

Keshav Kishore is currently serving as trainer at A P Goyal Shimla University, Shimla (H.P.). He is also serving as Associate Professor in the Department of Computer Science & Engineering. He has played vital role in the implementation of New IT-Labs and Web application Development for the various projects of the University. He is having 4 years of Industry experience at various levels. He is expert in FOSS; Application Development & Security Management. He is having more than 5 Years of academic and administrative experience in the field of Computer Science & Information Technology. He has published more than 14 research manuscripts in various International & National journals & conferences. He has also presented papers in International and National conferences. He is the member of various International & National professional & academic bodies. In addition to this, he is the member of various committees and BOS (Board of Studies). He has guided the students in their M. Tech dissertations. He is an active participant of various Seminars, Induction and faculty development programs.