Review the Types of Access Control Models for Cloud Computing Environment

Azlinda Abdul Aziz[1], Salyani Osman[2]
Department of Computer Science, Universiti Selangor, Selangor, Malaysia
[1]azlinda@unisel.edu.my
Department of Information Technology, Universiti Selangor, Selangor, Malaysia
[2]salyani@unisel.edu.my

Abstract--Cloud computing is the internet base models that enables cost reduction, on demand, scalability, flexibility, pay per uses access to pool of sharing resources. Cloud Computing enables to share the software, data, hardware and storage. Beside the advantages, many new issues have occurred in Cloud Computing and the main issues is the problem concerning to the access control. Cloud access control is a policy defined as a cloud security requirement that specific how the users may access specific resources. In access control, there are several rules must be followed before the users can access any kind of data or resources from the cloud computer. There are many existing access control models in cloud environment. This study aims to develop an access control model and techniques for higher learning institution. The objectives of the study are to design an access control model, apply the model in higher learning institution domain and evaluate it for model validation purposes. On literature reviews, the function of several types of access control models, their advantages and limitations of the models are discussed.

Keywords-Cloud Computing, Service Provider, Access Control, Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role Based Access Control (RAC, Attributed-Base Access Control Model (ABAC)

I. INTRODUCTION

Cloud Computing is an internet technology that cloud service provider enable to rent the storage, hardware, servers, application sand enable the data owner to store data that control by the service provider. Cloud computing used the distributed access control architecture that the entire authorize consumer can ease and fastest retrieve the data at all site.

Cloud Computing have three service model architecture, Software as a service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [1]. For SaaS uses common resources and a single instance of both the object code of an application as well as the underlying database to support multiple customers simultaneously such as web browser. While PaaS included all the system and environment comprising the end to end life cycle of developing, testing, deployment and hosting of sophisticated web application as a service delivered by a cloud base such as Java, Python and .Net. Where IaaS is computer infrastructure as a service which include operation system, storage and processing.

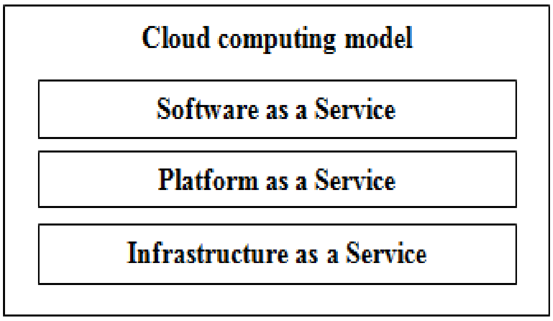


Fig. 1. Cloud Computing Model

Cloud Computing has three deployment model architecture [2]. Private cloud that data and processes are manage within the organization without restrictions of network bandwidth, security exposures and legal requirements Public cloud is the resources are dynamically provisioned on a fine-grained, self-service, from an off-site third-party provider who shares resources. Hybrid cloud the environment is consisting of multiple internal and external providers.

I. PROBLEM STATEMENT

When data are on a cloud, anyone can access it from any location. To make a right person can be access, modified and process the data. Access control algorithms should differentiate between a sensitive data and a common data otherwise anyone can access sensitive data. The vendor does not reveal where all the data are stored. Data may be located anywhere in the world, which may create legal problems over the access of the data. Data loss is a very serious problem in cloud computing while accessing data. If the vendor closes due to financial or legal problems, there will be a loss of data for the customers. The customers would not be able to access those data.

II. RESEARCH QUESTION

1. How to identify the classification of access control model in cloud computing?
2. What types of techniques are appropriate to identifying the secure access control models for higher learning institution?
3. How to develop an access control model and techniques for higher learning institution?
4. What type of validation process to evaluate the access control model and techniques for higher learning institution?

III. RESEARCH OBJECTIVE

1. To examine the classification models of access control
2. To determine the appropriate technique in secure access control in cloud computing for higher learning institution
3. To develop an access control model and techniques for higher learning institution.
4. To validate access control model and techniques for higher learning institution.

IV. CONTRIBUTION

The study to be reported potential contributions in the following ideas:

Theoretical and body of knowledge Implication This research contributes to the body of knowledge by amplifying the relatively scan research on access control mechanism. Some existing models will be explored and assist model development

V. PRACTICAL IMPLICATION

The contribution of this study is the access control model for higher learning institution, can be used as a means of guideline for accessing control in cloud computing.

VI. LITERATURE REVIEW

Access Control is a fundamental aspect of computer security that is directly tied to the primary characteristics such as confidentiality, integrity and availability [3]. There have 3 requirements for cloud services [4]:

Cloud service provider must be able to specific access control policies for user access data and resources. Data Owner must be able to offer cloud services to consumer.
An organization must be able to enforce more access control policies on its user requests for resources of the organization.
The cloud service provider wants to ensure that the resources and service are utilized only by the authorize user. Consumers would like to ensure the data is securely maintained in the cloud by the cloud service provider. Subject is the process requested by consumer or data owner and objects is a file, directories, share memory segment which control by cloud service provider.

Traditional Access Control Model cannot be applied directly in cloud environment because it is a static nature. A large amount of the resources, huge number of dynamic user, flexible and dynamic which should be considered in Access Control model for cloud computing. [5]
For example, to observed the user of a cloud at SaaS level, the services through the Internet using mobile phone, PDA and notebook. It is possible to identify using fix IP address of the user. In cloud users are normally identified by their attributes. It needs dynamic access control to achieve the cross-domain authentication.

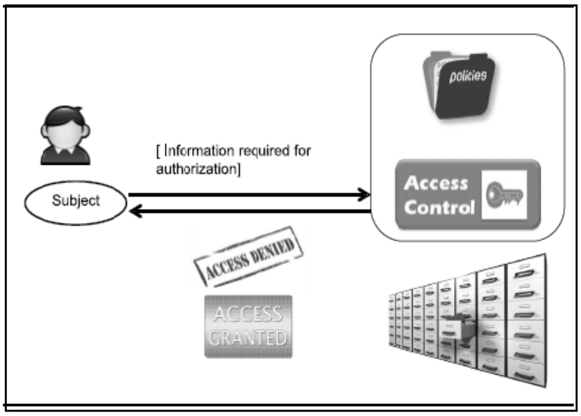


Fig. 2. Example of Access Control

A. *Access Control Models*

This section discusses the various types of Access control models for Cloud computing Environment.
Mandatory Access Control Model (MAC)

Mandatory Access Control (MAC)[6] enables user to the subject to access an object in the system. Each user, subject and object in the system is assigned with a security level [7]. The security level associated with an object reflects the sensitivity of the information contained in the objects. The policy set-up and management are performed in a secured network and are limited to system administrators in Mandatory Access Control [8].

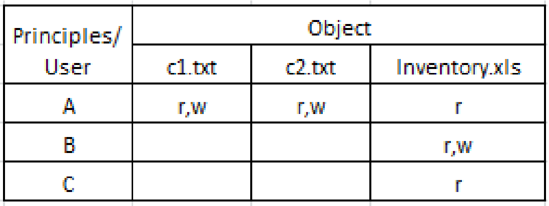
When a user attempts to access a resource under Mandatory Access Control, the operating system checks the user's classification and categories and compares them to the properties of the object's security label. If the user's credentials match the MAC security label properties of the object, access is allowed. It is important to note that both the classification and categories must be matched. A user with top secret classification, for example, cannot access a resource if they are not also a member of one of the required categories for that object.

The central administrator controls all the tasks and the administrator defines the usage and access policy, which cannot be modified by the user.

B. Discretionary Access Control Model (DAC)

Discretionary Access Control (DAC) [9] allows each user to control access to their own data. Each object on a DAC based system has an Access Control List (ACL) connected with it. An ACL contains a list of users and groups to which the user has permitted access together with the level of access for each user or group.

Figure 3 shows the User A may provide read-only access on one of her files to User B, read and write access on the same file to User C and full control to any user belonging to Group 1 [10]. The table entry for a principal P and an object O lists privileges corresponding to those operations on O that are authorized when invoked by execution being attributed to P. Execution attributed to any of the three users can read inventory.xls.



Principles/ User	Object		
	c1.txt	c2.txt	Inventory.xls
A	r,w	r,w	r
B			r,w
C			r

Fig. 3. Example of DAC policy

C. Role Based Access Control Model (RBAC)

Role Based Access Control Model (RBAC)[11] is determine the user to access the system and network by the job role. The RBAC is the ability of an individual user to access a specific task, such as view, create, or modify a file. It is defined the minimum amount of permission and functionalities that are necessary for the job to done [12].

For example, the role in the bank includes user, loan officer and accountant. Each user is associated with a set of roles which are assigned by administrators. Each role is associated with a set of permissions of the object. Users can create sessions in the system. The creating user is becomes the owner of the session and is the only one who can delete the session. When a user deletes a session, the association between the session and activated role is also deleted. A session is really equivalent to a subject. The owner of a session can activate and disable the roles that he is assigned in that session. User permissions in each session are determined by the set of activated roles within that session.

In Figure 4 is shown the relationship between user, roles (group) and system objects.

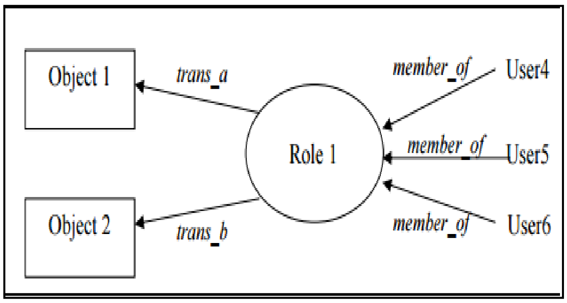


Fig. 4. Role relationship

D. Attributed-Base Access Control Model (ABAC)

Attributed-Base Access Control Model (ABAC)[13] more secure compare to the traditional public key to protect the privacy and secrecy of data in cloud computing environment. Attributes are characteristics of the subject, object, or environment conditions. Attributes contain information given by a name-value pair. ABAC are granted to users through the use of policies which combine attributes together. The policies can use any type of attributes such as user attributes, resource attributes, environment attribute and etc.

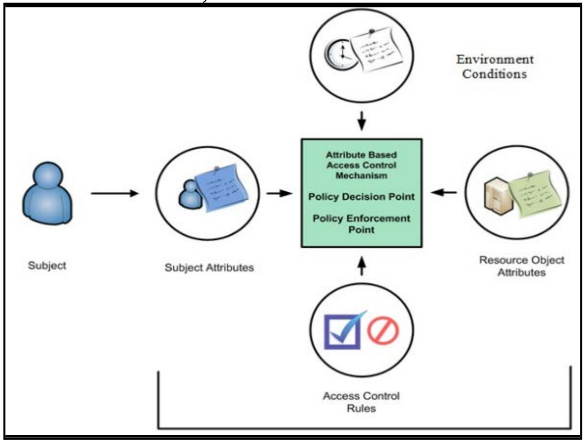


Fig. 5. Core ABAC Mechanism

When an access request is made, attributes and access control rules are evaluated by the attribute based access control mechanism to provide an access control decision. In Figure 5 is shown the ABAC's basic form, the access control mechanism contains both a policy decision point and a policy enforcement point [14].

The ABAC system is composed of three parties, namely data owner, data consumers, cloud server and third-party auditor, if necessary. To access the data files, shared by DO, data consumers or users can download the data files of their interest from the cloud server. After downloading, consumers decrypt the file. Either the data owner or the user will be online all the time. The ABAC provides policy for sensitive data. It allows an organization to maintain its autonomy while collaborating efficiently.

The ABAC is composed of four entities shown at Figure 6 [12]: Users are sending the request to the cloud and invoke action on the service. Service is the hardware and software in the cloud. Resources shared among the cloud services. If the data or resources not present in that cloud service, the resources will be get from another cloud service.. Environments that contain the information that is might useful for taking the access decision such as date and time.

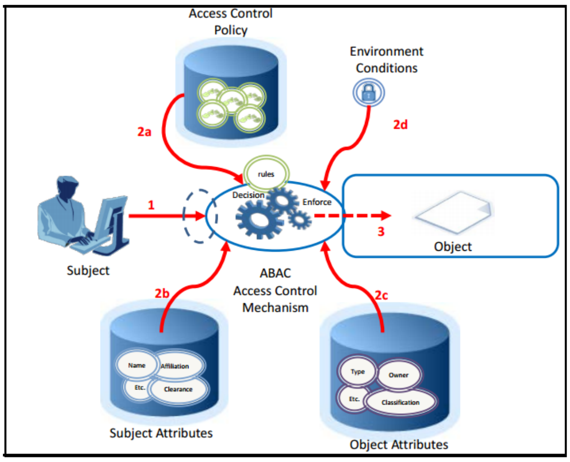


Fig. 6. Basic ABAC Scenario

E. Advantages and Limitations of the existing models

From these four access control model discussed, there are advantages and limitations of the each models. The advantages and limitations are shown at Table 1 and Table 2 below:

TABLE 1: ADVANTAGES OF MODELS

Model	Advantages
Mandatory Access Control Model (MAC)	MAC provides higher security because only a system administrator can access or alter controls.
Discretionary Access Control Model (DAC)	Object access is determined during access control list (ACL) authorization and based on user identification.
Role Based Access Control Model (RBAC)	Increased security of complex organization, reduce complexity and cost.
Attributed-Base Access Control Model (ABAC)	ABAC add additional parameters such as resource information, requested entity, resource and dynamic information such as time and user IP.

TABLE 2: LIMITATION OF MODELS

Model	Limitations
Mandatory Access Control Model (MAC)	MAC is central administrator and it does not ensure fine-grained least privilege, dynamic separation of duty and validation of trusted components.
Discretionary Access Control Model (DAC)	DAC doesn't scale well the on systems with large number of subject and object
Role Based Access Control Model (RBAC)	Across extended administrative domain of an organization
Attributed-Base Access Control Model (ABAC)	Does not provide data scalability and confidently simultaneously

REFERENCE

[1] NIST, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology," Nist Spec. Publ., vol. 145, p. 7, 2011.

[2] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing : state-of-the-art and research challenges," pp. 7–18, 2010.

[3] S. Sinclair, "Access Control In and For the Real World," 2013.

[4] A. Majumder, S. Namasudra, and S. Nath, "Taxonomy and Classification of Access Control Models for Cloud Environments," pp. 23–33, 2014.

[5] N. Meghanathan, "Review Of Access Control Models For Cloud Computing," Comput. Sci. Inf. Technol. (CS IT), vol. 3, no. 5, pp. 77–85, 2013.

[6] C. Zhang, Y. H. U. G. Zhang, and P. R. Chin, "Task-Role Based Dual System Access Control Model," J. Comput. Sci., vol. 6, no. 7, pp. 211–215, 2006.

[7] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," 2012 Int. Conf. Comput. Sci. Electron. Eng., no. 973, pp. 647–651, 2012.

[8] A. Majumder, S. Namasudra, and S. Nath, "Taxonomy and Classification of Access Control Models for Cloud Environments," pp. 23–33, 2014.

[9] L. Popa, M. Yu, S. Y. Ko, S. Ratnasamy, and I. Stoica, "CloudPolice: taking access control out of the network," Proc. Ninth ACM SIGCOMM Work. Hot Top. Networks, no. 1, pp. 1–6, 2010.

[10] F. B. Schneider, "Access Control Chapter 7 Discretionary Access Control," Draft Chapters, 2012.

[11] S. Kunz, S. Evdokimov, B. Fabian, B. Stieger, and M. Strembeck, "Role-based access control for information federations in the industrial service sector," Eur. Conf. Inf. Syst., pp. 1–12, 2010.

[12] D. F. Ferraiolo, J. F. Barkley, and D. R. Kuhn, "Role-Base Access Controls," ACM Trans. Inf. Syst. Secur., vol. 2, no. 1, pp. 34–64, 1992.

[13] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based Encryption for Fine-grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Comput. Commun. Secur., pp. 89–98, 2006.

[14] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to role-based access control," Computer (Long. Beach. Calif)., vol. 43, no. 6, pp. 79–81, 2010.

[1]