A Survey on Access Control Models and Applications

Nancy Ambritta P.
STES' Sinhgad Institute of Technology and Sciences
Department of Computer Engineering
Narhe,Pune,India

Yogita S. Hande
STES' Sinhgad Institute of Technology and Sciences
Department of Computer Engineering
Narhe,Pune,India

Santosh A. Darade
STES' Sinhgad Institute of Technology and Sciences
Department of Computer Engineering
Narhe,Pune,India

ABSTRACT
Access control, as the name indicates is a security measure that regulates access to resources/confidential data by verification of access rights (credentials) of users. This paper is a survey of the existing access control mechanisms that enables a novice reader to understand the existing concepts and models, analyze their usage and limitations in order to develop better mechanism by building up on the existing models that will better adapt to meet the changes/advancements in technology. The study will further enable the development of a strong and attack resilient access models that are eventually the need of the hour.

General Terms
Access Control Methods

Keywords
Access Control; Mandatory Access Control; Discretionary Access Control; Role-based Access Control; Rule-based Access Control; Content-based access control.

1. INTRODUCTION
Access control is a technique that enables us to emphasize a selected restriction on access to data/privileges to authorized users. Therefore, identification, authentication (audit/verification against predefined policies/rules) and authorization are the three major activities that make up an access control model. Access control mechanism allow subject (user) to use their credential to identify themselves as legitimate users and help gain access to resources. A simple and well known application of this access control is its usage in Linux systems wherein users are regulated access to files based upon a predefined Access Control List (ACL). This paper further highlights a few areas where access control is applied and how it is put to use. It also defines a scenario to depict one such usage followed by a short survey of the existing access control models.

2. ACCESS CONTROL APPLICATION AREAS
Access control finds its application in various areas. The most significant and unavoidable area of application is the Internet of Things. Internet of Things is a convergence of various technologies like the cloud (for its storage, resources and computational capacities), fog computing, cyber physical systems and many more. It involves the connection of devices/things intermittently over the internet. With this continuous connectedness and exchange of information comes the need to protect the data from unauthorized access. In this regard, access control comes as our first line of defense,

wherein specific rules are verified by trusted parties in order to regulate access. A few scenarios that explain the application of access control are explained further.

The most important and vital need of having a well built access control mechanism is in the hospital/clinical management system [1] wherein sensitive patient information should be available only to the appropriate doctors/users to ensure the safety and privacy of the patient. Also, in times of life critical situations wherein a patient needs to be treated by a doctor remotely, regulating access to the patient's records by application of proper access control mechanisms is of utmost importance.

Access control finds its application in other scenarios such as smart home implementation, automotive technologies and the like. Smart homes involve devices that need to interact with each other for an organized execution of tasks. Also, the need to identify the appropriate users/owners who access the internal devices and manipulate their functionality is of prime importance that ensures the safety of the authorized users belongings.

Access control being the first line of defense, if not implemented with utmost care, itself, suffers from severe security risks that hamper the privacy and confidentiality of user's personal information or a specific group's data [2]. This hampering of functionality could be due to the various loop holes in security that exist as attacks namely the spoofing attack, collusion attack , man-in-the-middle attacks and so on. Having said that developing an attack resilient access control model that fits good into the evolving technological world by adopting the pros in existing mechanisms and developing remedial models that address the security risks is the goal that needs to be achieved that would help access control find a better suitable place in today's world.

Figure 1 represents a hospital management scenario wherein the patient records are contained in a central database [3]. Every patient record (PRn) is guarded against illegal access by deploying access policies. Only legitimate practitioners/doctors and patients (access only personal records) are allowed to access the appropriate records while they are deprived of access to other patient's records thereby ensuring the security and privacy of patient's records. Proper verification of credentials by the trusted entity that appliesaccess control audit is required in order to ensure the success of this system.

However, the implementation of security at the system level places restrictions on user actions thereby preventing any dynamic decision making in alteration of policies.

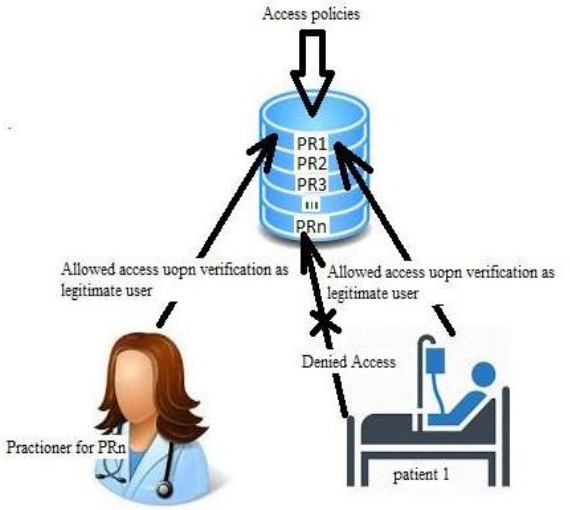

Fig 1: Access Control Application in hospital/clinical management system

3. LITERATURE REVIEW

Access Control is an important mechanism which protects system resources and also helps different applications to give specific resources/object access to subject/user. There are two main Types of Access Control:

a) Physical Access Control: Physical Access control system designed to control the physical attribute. Example like access control to room, building and campus.

b) Logical Access Control: Logical Access Control system designed to control the computer network system. Example like local access control to number of connection to computer, files and data.

Access Control categorizes into seven different types as shown in figure 2.

3.1 Mandatory Access Control

The Access Modular Controller (AMC) follows the hierarchical approach to assign privileges to resource objects. The MAC model for computer security allows subject access to all resource objects controlled by operating system based on system administration configured setting. Under the MAC subject cannot change the control list designed for resources [4].

A subject is allowed access the object based upon security labels with policies determined by network administrator enforced by operating system. Special UNIX operating systems are based on MAC. MAC is generally applied in environments where security rules are definite and security strategy is simple. MAC is mostly used in government and military field by assigning a classical label to file system object. In MAC since users do not have the control over the access policy applications and declassify information, the system is safeguarded from the Trojan horse attacks.

3.2 Discretionary Access Control

DAC access control type defined by Trusted Computer Evaluation Criteria. In DAC the owner of the resource objects (file and data) grant access through policy determined. Simple example of DAC in UNIX operating system, file mode like read, write and executable permissions assigned to every user, group and others. In DAC [4] Access Control List (ACL) consists of a list of subjects with their permission to access the file on that operating system.

Lower lever DAC in contrast with MAC, does not allow resource owner to assign access control and to prepare their own policies [5]. DAC is "need to know" access model. It helps realize the principle of least privilege wherein the user is allowed to access just the right amount of information (nothing more, nothing less) based upon his credentials. DAC provides the flexible environment to access the resources. The discretionary access control and mandatory access control are mostly used in secure operating systems. However, placing the user in control poses a threat of exposing the system to Trojan horse attacks.

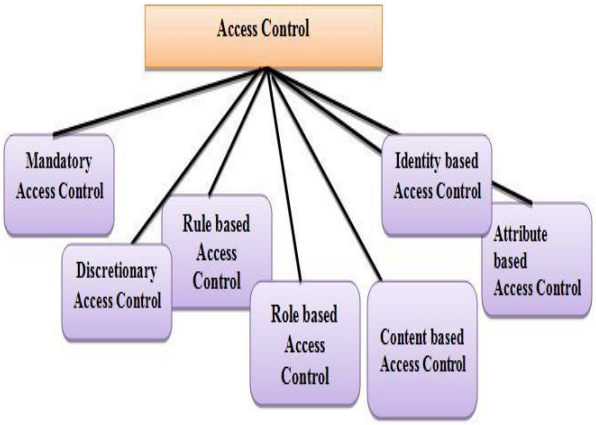

Fig 2: Access Control Models

3.3 Role-Based Access Control

Most of the enterprises and organizations go with Role based access control because the privileges to objects are based on roles of employees in the organization. Computer applications are always in developing mode, computer security changes continually but DAC and MAC support only some access control demands [4]. Role is defined based on responsibility, authority and job within the enterprises. Subject user inherits privileges that are tied with their role hence it is called Non-discretionary Access Control. The main advantage of RBAC is that roles can be easily created and can be changed as per requirements of enterprise, thereby making management of policies easier. However, the consolidations of many users into one group prevent the ability to apply fine-grained access policies to realize a customized access control environment.

3.4 Rule-Based Access Control

The Rule based access model allow system administrator to access or deny the resources object to subject. In discretionary access control model, ACL is implemented by Network administrator for user or group. If any user or group is accessing the object, operating system checks the rule contained in ACL for that object. Example of Rule based access controls are situations in which any account or group can access the network connection at certain hours or days of the week.

3.5 Content-Based Access Control

It is an innovative access control model designed for content centric information sharing. It is applied where RBAC will give more access right; on top of such model CBAC is deployed [6]. The CBAC model takes access control decisions based on content similarity. In CBAC subject can use RBAC model to access all large set of objects but CBAC add

additional restriction to subject where the subject could access subset of designated record. Boundary of the subset is dynamically determined by the textual content of data objects

3.6 Identity-Based Access Control

Identity based access control is the general mechanism that exists for authenticating a device/user based on the identity or password that they possess. It provides a mechanism for identifying who the user is. A variation of this is the group identity access control that enables access to a group of users gain access to databases and the like resources. A simple example of identity based access control is the secured access to wifi networks

3.7 Attribute-Based Access Control

Attribute based access control provides access to users by verification against access policies that are formed by combining relevant attributes to regulate access to users [7]. This provides a mechanism to enable fine grained access to resources/data. It helps realize the most need 'principle of least privilege' to ensure the security of resources and information that is contained in the system. A simple example that follows attribute based access control is where access to specific company related data are provided to employees who have completed 15 hrs of training on a specified platform.

4. CONCLUSION AND FUTURE WORK

Access Control is interpreted as controlling access to a system from external resources. In this paper we discussed access control concepts with application and types. Different access control types model provide privileges to object in specific way which allow subject to restrict the resources access to user. Identification of the most suitable access control mechanism for a particular area is an important and critical decision to be made, that would lay the basis for the security of the resources and contained information. Our future scope is to apply the existing access control models (hybrid models) and build upon them so as to meet the current demands in upcoming technological areas.

5. REFERENCES

[1] Khan, M.F.F.; Sakamura, K.," Context-aware access control for clinical information systems", International Conference on Innovations in Information Technology (IIT), IEEE, pp.123 – 128, 2012 .

[2] http://www.agiledata.org/essays/accessControl.html

[3] Min-A Jeong, Jung-Ja Kim, Yonggwan Won, " A flexible database security system using multiple access control policies", International Conference on Parallel and Distributed Computing, Applications and Technologies, IEEE, pp-236-240, 2003.

[4] BAI Qing-hai, ZHENGYing, "Study on the Access Control Model in Information Security", Cross Strait Quad-Regional Radio Science and Wireless Technology Conference, IEEE, pp. 830-834, 2011.

[5] Yanfang Fan, Zhen Han, Jiqiang Liu, Yong Zhao, "A Mandatory Access Control Model with Enhanced Flexibility", International Conference on Multimedia Information Networking and Security, IEEE, pp.236-240, , 2009.

[6] Wenrong Zeng, Yuhao Yang, and Bo Luo. "Content-Based Access Control: Use Data Content to Assist Access Control for Large-Scale Content-Centric Databases," IEEE International Conference on Big Data, IEEE, pp. 701-710,2014

[7] https://www.jerichosystems.com/technology/abac.html