International Journal of Computer and Communication Technology

Volume 4 | Issue 2 Article 7

April 2013

Towards Authentication and Authorization – Electronic Medical Records

Pallavi Kalambe
Deptt. of Computer Science & Engineering, Shri Vaishnav Institute of Science & Technology, Indore, India, kalambe.pallavi@gmail.com

Rajeev G. Vishwakarma
Deptt. of Computer Science & Engineering, Shri Vaishnav Institute of Science & Technology, Indore, India, Rajeev@mail.com

Recommended Citation
Kalambe, Pallavi and Vishwakarma, Rajeev G. (2013) "Towards Authentication and Authorization – Electronic Medical Records," *International Journal of Computer and Communication Technology*: Vol. 4 : Iss. 2 , Article 7.
DOI: 10.47893/IJCCT.2013.1178
Available at: https://www.interscience.in/ijcct/vol4/iss2/7

Available online at www.interscience.in

Towards Authentication and Authorization – Electronic Medical Records

Pallavi Kalambe & Rajeev G. Vishwakarma
Deptt. of Computer Science & Engineering, Shri Vaishnav Institute of Science & Technology, Indore, India
E-mail: kalambe.pallavi@gmail.com, Rajeev@mail.com

Abstract **-** The Technological intervention in field of Computer Science and Information Technology has made it possible to access medical records of Individuals electronically. Electronic Health Records systems which are distributed and need to be interoperable too. Important Business drivers for such kind of high level of interoperability introduce unique citizen ID. Though citizen have access to data from central repository and they can directly communicate with health care providers, but when it comes to security and confidentiality, technology fails to meet the requirements. In this paper we suggest a framework for authentication and authorization of Electronic medical Records System in consideration .It will help to build An Secure-Privacy Protected Electronic medical Record System.

Keywords— *Electronic Medical Records, Authentication, Authorization.*

I. INTRODUCTION

Sharing and proper use of confidential information is very important aspect of EMR (Electronic Medical Record) System. EMR integrates all relevant medical information of a person and represents a lifelong documentation of his medical history. Due to sensitivity of medical details, it is crucial to manage those details in such a manner that it can only be accessed by the patient themselves and medical practitioners who are directly involved in the treatment of the patient, Since various portals which are supporting electronic medical records can be accessed via the Internet, security and privacy issues arise that have to be considered carefully and should be handled properly. [1]

Information privacy typically concerns the confidentiality of personal identification and protected health information. Thus, privacy and security for information access control mechanism for e-Health services must be developed in such a way to provide proper security and confidentiality.

Access control is the mechanism of limiting access to the resources of a system to authorized users. In general, access control can be defined as the process by which users get permission to access to resources, on the basis of authentication and associated privileges authorization .[2]

Various models and techniques have been designed and developed to solve the problem of organization's authorization requirements but when it comes to individual privacy, all fail to meet. [60]

There are some very well established Access control mechanism like Discretionary Access Control, Mandatory Access Control and Role Based Access control .these are designed according to industry standard.[3] Discretionary Access Control (DAC) is the very first standard which enables and controls the information access on the basis of user's identity and authorization[4]. Mandatory Access Control (MAC) was designed to overcome limitations of DAC, enables and controls the information access on the basis of security classification of users and objects in that particular system. The Role Based Access control is the third standard which regulates information access on the basis of activities that can be performed by particular type of user in the system.

This paper demonstrates all three information access mechanisms DAC, MAC and RBAC from the perspective of EMR .then we explain that in isolation each of them will not be sufficient for fulfilling security and privacy demands but if all three are combined together then only they will be able to deliver necessary information access control mechanism. We have also presented a conceptual model of their proper combination.

II. RELATED WORK

To restrict all those illegal activities which can be performed by some unauthorized or unauthenticated user, control mechanism should be developed...in last two decades several mechanisms have been established which are described here [4]:

2.1 DISCRETIONARY ACCESS CONTROL

The mechanism involves restriction for accessing objects, and it is based on identity of group to which they

belong. Here the identities of the user act as the key to DAC although it is widely being used but even then there two things which makes it weak:

1. Granting read access is transitive. For example when Sara grants Bob read access to a file, then Bob can copy its contents to some another file and now onwards Bob may grant other user to access to copy of Sara's file without Sara's knowledge.
2. DAC policies are vulnerable to "Trojan Horse" attack, because programs inherit the identity of the invoking user, Bob; for example, write a program for Sara that, on the surface, performs some useful functions, while at the same time it destroys the contents of Sara's files.

Sub/Obi	RECORD 1	RECORD 2	RECORD 3
Cherry	Read,w,ex	-	write
John	-	write	Read,w,ex
Fred	-	Read,w,ex	read

Table 2.1: Access Control Matrix

Access control matrix is a popular model in access control area, which applies DAC policies. The basic function of an access control sister is to only those operations can be executed which are specified in matrix. There are two primary representations of the access matrix which are Access control list and capability list. Access control list is attached to an object and specifies which subjects may access the object while a capability list is attached to a subject and specifies which objects can be accessed by the subject.

When it comes in field of electronic medical recors, DAC model can be implemented where medical practitioners and patients are users, patient's medical details and records are objects and all those actions which are allowed for users will be operations such as read and write. However there are some security and confidentiality related issues that make DAC inappropriate to be implemented in EMR systems [5].

1. In EMR there is no single owner of data (there are medical practitioner, patients, management authorities) so it contradicts DAC's data owner assumption.
2. Whenever there is a need of complex access control requirements ("need to get details") in EMR, it cannot be accomplished by DAC.

2.2 Mandatory Access Control

This mechanism is known for preventing "Trojan Horse" problem that occurs in DAC[66,136].here decisions related to access policy are made by a central authority, not by the individual owner of data or object, and owner cannot change access rights.MAC does not gives user full access control over resources they created. Determination of access controlling is done on the basis of security libeling mechanism. [143]For example a user who is authorized to access the part "Secret" is not allowed to access the part "Top Secret" of classification. This is known as "No Read Up". And in same way "No Write Down".

In EMR systems various MAC security levels could relate to different type of health care employee (doctors, Nurses, receptionist, etc).so it might be very difficult to use MAC mechanism in EMR systems that huge number of users participate in system, the wide range of data types and the desire to give partial access control of medical records.

2.3 Role- Based access Control

RBAC decisions are done on the basis of the roles that individual user has in particular organization [66].different roles are assigned to each one of organization and respective access rights are grouped by role name. Access of that particular resource is limited to authorize users only.

Figure2.3.1: RBAC relationships

Role based Access control Model taxonomy consists of four models [79]:

1. Core RBAC: covin the basic set of features that are included in RBAC.
2. Hierarchical RBAC: use the concept of hierarchy and inheritance.
3. Static constrained RBAC: static separation of duty. (Same user cannot perform given roles).
4. Dynamic constraints RBAC: achieved by enforcing the control at access time [9].

RBAC model lakes the ability to incorporate other access parameters or contextual information that are information access to user[3,6,10].for example, In life critical emergency cases when doctors must have access to a patient's EMR even if he has not been given the patient's consent. This poses the need to modify the RBAC to accommodate these limitations.

III. AUTHORISATION REQUIREMENT IN EMR ACCESS CONTROL

A control mechanism for electronic medical record access must satisfy all EMR participants'' needs, i.e. patients, medical practitioners and medical authorities.

Here are those requirements which are crucial to healthcare environment:

1. Patients should have the rights to have control over their own health records, including whether or not to grant access to certain medical practitioners [9, 10, and 11].
2. Patients should be able to hide specific items of information from their EMR from selected medical practitioners [5].
3. Patients should have the ability to delegate privacy control over their EMR to other users under certain conditions (e.g. mental illness) [8, 5].

IV. COMBINED ACCESS CONTROL PROTOCOL

In this model, access to a particular EMR is granted only if it satisfy all three access control policies. The challenge is to determine where and how each of the access control constraints introduced.

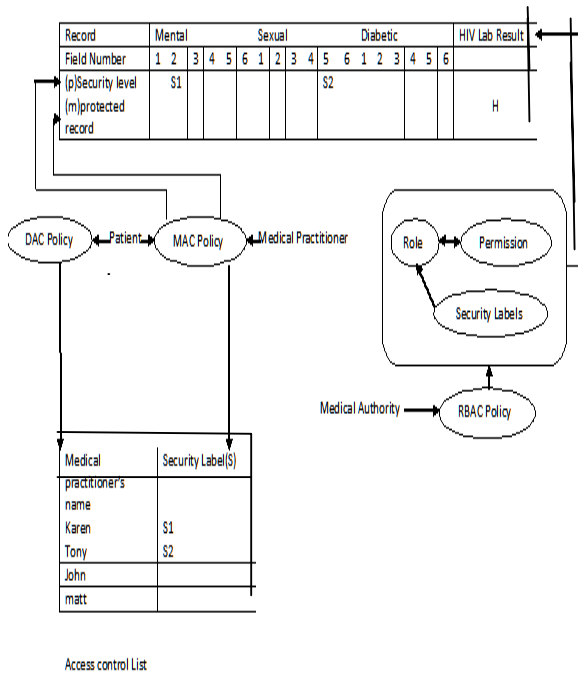

Figure 4.1: the Logical Structure of combined Access Control protocol

The basis of our protocol is shown in figure 4.1 an electronic medical record schema is shown where each field has two MAC based security labels: one positive label (p) is assigned by the patient and the second is negative label (m) assigned by medical practitioner.

These labels are used to express the sensitivity class of data field. Also a DAC access control list is maintained by the patients, whereby they nominate their trusted medical practitioners and set the positive security labels for each of them. This security label allows a medical fractioned to access sensitive data that may not be allowed for other medical practitioners. Access to EMR is further restricted by an overall RBAC based access control policy managed by the medical authority.

Now when it comes to patient's privacy requirements, whereby patients want to decide who is authorized to access their electronic medical records, to determine what is sensitive information in their EMR detail and who is authorized to access it, these requirements are satisfied by executing following steps using DAC and MAC interface in our combined access control policy:

1. Patients nominate the names of medical practitioners via DAC.
2. With the help of MAC they will be able to categorize sensitive information.
3. To allow specific medical practitioners to gain access to security classified data in patient's EMR, the patient via MAC interface assign positive security label of sensitive data field to authorized medical practitioners' access control list.

Medical practitioners' access control requirements are also satisfied here in following manner:

1. Medical authority defines roles, permissions and role-permission assignments via RBAC interface. This process is done by domain experts who know the access requirements for each medical role. Therefore the "Need to know" principle is achieved and medical practitioners' access needs will not be limited unless the patient has set some additional access control restriction through DAC or MAC interface.
2. Since RBAC can incorporate contextual attributes into role assignment, it would be possible for a medical practitioner to have both an access role as GP in a day clinic or as a GP in an emergency department. To allow the GP in an emergency dept to access the required medical data, including the patient's security-classified data records, the RBAC policy assigns a security label to these critical roles to allow medical practitioners access to secure data.

V . CONCLUSION

Authentication and authorization provisions provided for accessing the information in EMR, but here in study, we showed that none of three standard access control model, DAC, MAC and RBAC are adequate for EMR system in isolation. Here we explained how a careful combination of all three access control models can provide the privacy requirements needed for an EMR system.

However I isolation we assume that patients are able to adequately understand and manage access to their EMRs. We assume that a medical authority will be responsible for determining what medical data that patients are allowed to have control over in order to ensure the patient's EMR will present the required information that a medical practitioner needs to do his medical job. In our work to date, we have not yet validated the security of our model by accessing it against adversary models, e.g. a malicious healthcare worker. However this work can be carried out as an extension to the work presented here.

REFERENCES

[1] Privacy Aspects of healthy Daniel Slamanig and Christian Stingl 2008 The Third International Conference on Availability, Reliability and Security.

[2] Privacy Access Control Model for Aggregated e-Health Services Patrick C. K. Hung and Yi Zheng 2007 Eleventh International IEEE EDOC Conference Workshop (EDOCW'07)

[3] B.Finance, S Medjdoub and p.pucheral. privacy of medical records:from law principles to practice.Proceedings of the 18th IEEE symposium on Computer-basedmedical System,Dublin,23-24 June 2005

[4] R.S Sandhu and P.Samarati. Access Control: principles and practice. IEEE communication magazine 1994

[5] CSIS, "Security Glossary," Information Systems Security Organization, 2003. Online: http:// ise.gmu.edu/~csis/glossary/merged_glossary.html

[6] D. F. Ferraiolo, D. R. Kuhn and R. Chandramouli,

"Role-based access control," Computer Security Series, Artech House Publishers, 2003.

[7] S. Osborn, R. Sandhu and Q. Munawer, "Configuring role-based access control to enforce mandatory and discretionary access control policies," ACM Transactions on Information and Systems Security (TISSEC), vol. 3, no. 2, 2000.

[8] E. D. Schoeman, "Philosophical Dimensions of

Privacy: An Anthology," New York, NY, Cambridge Univ. Press, 1984.

[9] H. Leino-Kilpi, M. Valimaki, T. Dassen, M. Gasull, C. Lemonidou, A. Scott and M. Arndt, "Privacy: A review of the literature," International Journal of Nursing Studies, vol. 38, pages 663-671, 2001.

[10] S. Fischer-Hubner, "IT-Security and Privacy," LNCS 1958, 2001.

[11] C. S. Powers, P. Ashley and M. Schunter, "Privacy promises, access control, and privacy management.

❑❑❑