Access Control for Healthcare using Policy Machine

Zahid Pervaiz, Arjmand Samuel, David Ferraiolo, Serban Gavrila, Arif Ghafoor

Abstract

Access control policies in healthcare domain define permissions for users to access different medical records. Role Based Access Control (RBAC) helps to restrict medical records to users in a certain role but sensitive information in medical records can still be compromised by authorized insiders. The threat is from users who are not treating the patient but have access to medical records .We propose selective combination of policies where sensitive records are only available to primary doctor under Discretionary Access Control (DAC). This helps not only better compliance of principle of least privilege but also helps to mitigate the threat of authorized insiders disclosing sensitive patient information. We use Policy Machine (PM) proposed by NIST to combine policies and develop a flexible healthcare access control policy which has benefits of context awareness and discretionary access. Temporal constrains have been added to RBAC in PM and after combination of Generalized Temporal RBAC and DAC an example healthcare scenario has been setup.

Keywords

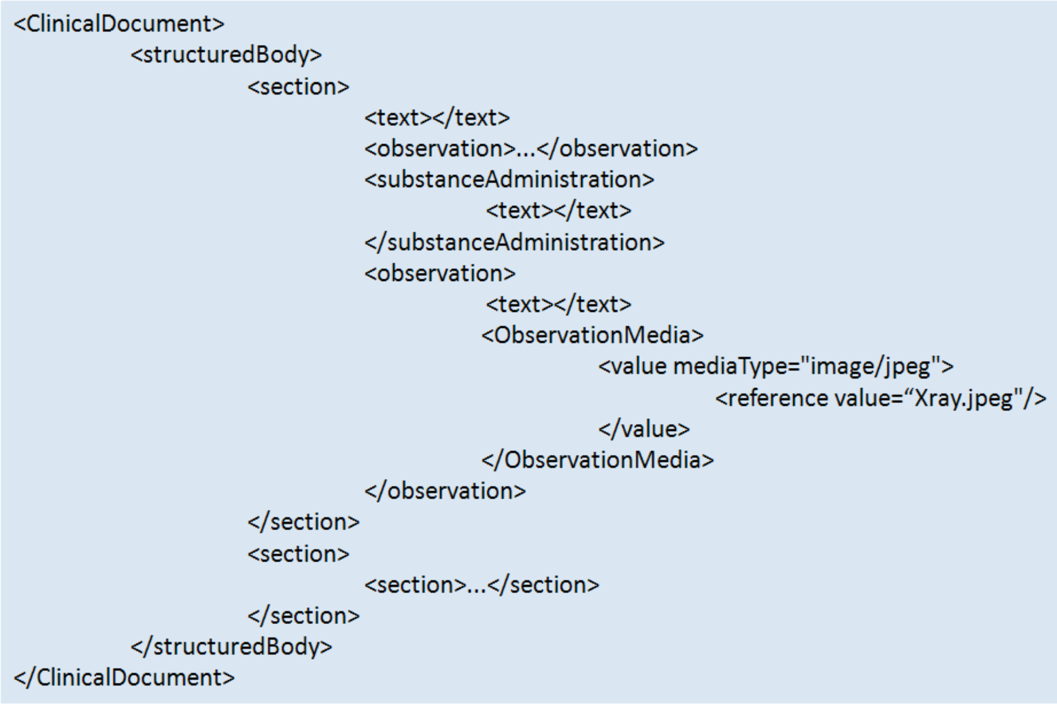
Access Control, Healthcare, Privacy, Role-Based Access Control

1. Introduction

Healthcare data of a patient contains sensitive information which requires enforcement of confidentiality mechanisms on healthcare records to protect the privacy of patients and to prevent access from unauthorized persons. Example of sensitive information in health records can be details regarding fertility and abortion, emotional and psychiatric problems, HIV and sexually transmitted diseases, physical and substance abuse. Protection of medical records becomes more important in cases where disclosure of personal medical information may create embarrassing situation for patients or causes discrimination based on medical ailment [1]. It is estimated that during a typical hospital stay, about 150 people like doctors, nurses, X-ray technicians, and billing clerks can access patient's medical records to perform their duties [2]. But in one incident, test results of a star baseball player were looked at by nearly 7000 people when he was under treatment at a New York City hospital for a shoulder injury [2]. In other incidents more than 120 workers at UCLA Medical Center looked at celebrities' medical records and other personal information without permission between January 2004 and June 2006 [3] and a New Jersey hospital suspended about 27 workers for peeking at records of actor George Clooney [4].

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the US Congress in 1996 which contains privacy and security rules to regulate the use and disclosure of Protected Health Information (PHI) [5]. PHI includes health information in any form or media that can be used to identify a patient. The privacy rule in HIPPA requires that if a health care facility discloses any PHI after authorization from patient then it should disclose only the minimum necessary information required to achieve its purpose.

Medical records are now maintained in many healthcare facilities in digital form known as Electronic Healthcare Records (EHR) or Electronic Medical Records (EMR). Clinical Document Architecture (CDA) prepared by Health Level Seven (HL7) is an American National Standards Institute (ANSI) certified standard [6]. HL7 standards are used in most of the healthcare facilities in US. CDA defines XML architecture for clinical documents and can include text, sound, images and videos. A CDA document has two parts, header and body. Header contains the information about patient and medical providers, while the body is divided into sections containing clinical information. Figure 1 shows a typical instance of XML CDA document. Here <ClinicalDocument> is the root element of the CDA schema and <structuredBody> element encapsulates the body of CDA document.



```
<ClinicalDocument>
            <structuredBody>
                        <section>
                                    <text></text>
                                    <observation>...</observation>
                                    <substanceAdministration>
                                                <text></text>
                                    </substanceAdministration>
                                    <observation>
                                                <text></text>
                                                <ObservationMedia>
                                                            <value mediaType="image/jpeg">
                                                                        <reference value="Xray.jpeg"/>
                                                            </value>
                                                </ObservationMedia>
                                    </observation>
                        </section>
                        <section>
                                    <section>...</section>
                        </section>
            </structuredBody>
</ClinicalDocument>
```

Figure 1. Example of a CDA Document [6]

In this paper we propose design of access control policies to protect sensitive data of patients in healthcare domain using Policy Machine. Our contribution is to show that policies like Discretionary Access Control (DAC) and Role Based Access Control (RBAC) have limitations for protection of sensitive data against insider threat and how better access control policies can be designed by selectively combining Generalized Temporal RBAC and DAC. The paper is organized as follows, in Section 2 we discuss the problem of insider threat in healthcare domain in terms of authorization and how it can be mitigated. In Section 3 different approaches for access control are introduced. We discuss and compare different access control mechanisms in Section 4. In Section 5 we discuss the healthcare application designed with PM. An example healthcare scenario is setup in Section 6 and Section 7 concludes the paper.

2. Insider Threat

Healthcare providers are expected to ensure privacy of patient health records. Different users like doctors, nurses and admission clerks may be required to access patient information to perform their jobs. The sensitive information can still be compromised within the security policy by authorized users if they are over privileged and are careless or have mal intent. The threat to confidentiality of information caused by misuse of privileges by authorized users is known as insider threat and level of misuse has been classified in [7] as follows

2.1 Types of Insider Threat

- **Carelessness or Unintentional**: This type of insider threat occurs when users forget to logoff properly or by mistake open the records of some other patient. The users may be inclined to take short cuts like not logging off intentionally if the authentication system is cumbersome. The behavior of users to keep their login id and password at some convenient place like around computer monitor, in drawers or on table in their work area can also be termed as carelessness and can result in compromise of their id and password. This threat becomes more profound if we consider the scenario where sensitive data of patients is available to all users [1, 2]. In this case the sensitive data of all patients is compromised even if login id and password of only one doctor has been stolen.

- **Curiosity**: It is assumed that users will access health records of patients under their care only. The audit mechanisms are usually in place to record any such access but still users due to curiosity might snoop in medical records of ex-relations, celebrities and colleagues.

- **Mal Intentions**: The authorized users might access personal information to harm or embarrass any patient or to earn profit by selling the information. Any employee may even take these actions to embarrass the healthcare facility if he is fired from the job.

The misuse of authorization by insiders in examples [1, 2, 3, and 4] is due to violation of principle of least privilege. This principle requires that a user be given only those privileges that are necessary to perform the specific job. It is violated when for ease of use the users are given permissions more than their requirement. Use of RBAC in healthcare domain for access control does allow to restrict the permissions for a certain role but still these permissions can give more information than required in case of sensitive data which can result in disclosure of sensitive patient information.

2.2 Approach to Mitigate Insider Threat

It is suggested that the healthcare data be classified as normal or sensitive. Sensitive medical data should be the one, disclosure of which will cause embarrassment or discrimination to the patient. The patient's privacy is compromised by leakage of sensitive medical information so he or she should be the one to make the decision to declare the information as sensitive. If patient classifies some information as sensitive then this should only be available to the doctor treating the patient. This doctor will then exercise control over sensitive data and may allow discretionary access to other users on need to know basis.

The insider threats to confidentiality of information can be mitigated by using access control mechanisms like DAC and RBAC. But both of them if used alone have some limitations for protection against insider threat which can be removed by selective combination of these policies. We suggest that the access to sensitive medical records of patients should be restricted to primary doctors only and is shared on need to know basis. This can be achieved by applying DAC policy to sensitive documents and RBAC for the normal documents. By comparing two scenarios, one where a person in specific role can see information of all patients to second where normal medical records are available for all patients but sensitive records are available only to primary doctor we will see how the threat of misuse by insiders is mitigated.

- Carelessness or unintentional: If a session of an authorized user has not been locked or the login id and password has been stolen then the sensitive information of the patients under treatment with that specific doctor will be compromised only instead of all patients.
- Curiosity: The curious insider is now restricted to just the normal information of all patients and the sensitive information of patients authorized to him only.
- Mal intentions: To harm or embarrass any patient the insider will need the specific sensitive information which is now available to primary doctor only and is denied to others.

3. Related Work and Access Control Background

Access control mechanisms for healthcare have been proposed to implement security and privacy policies. These efforts are based on extending RBAC to formulate privacy and security policies. Rafae et al have proposed XML based Generalized Temporal Role Based Access Control (X-GTRBAC) for healthcare and have designed an example policy based on requirement use cases [8, 9]. Most of the schemes proposed for healthcare in recent literature use RBAC [10]. Bandar et al have suggested combination of DAC, RBAC and MAC to satisfy access control requirements for Electronic Health Records [11]. The authors suggest combination of all three policies simultaneously which is a rigid requirement for healthcare scenario. For example sensitive data can only be given one label to have it available to a specific doctor under MAC. This will prevent sharing of the health records among doctors for tasks like consultancy. We propose a flexible approach where according to requirement sensitive records may be placed in one policy or both the policies. Also authors suggest that ownership of documents be with patients in DAC. We feel that although patients own the data and they should have access to all their records but ownership under DAC policy when applicable should be with the primary doctor who should be able to share it after getting permission from patient.

Hippocratic databases have been developed for protection of personal information. The basic theme is that data collection and disclosure should be associated with purpose specification and user consent. The authors propose Platform for Privacy Preferences (P3P) or the Enterprise Privacy Authorization Language (EPAL) for policy specification. The Hippocratic databases are designed to enforce better disclosure policies so that patient preference is taken into account while sharing health information with research organizations, pharmaceutical companies or government agencies. The database also has an audit mechanism to find security breaches but in case of insider threat the goal should be to protect the information in first place instead of finding the culprit after the damage has been done [12, 13, and 14]. The exception based mechanisms are part of healthcare to allow access in case of emergency but it was observed in [15] that the use was too frequent to detect any misuse. Most of the exceptions have been in case of referrals and second opinions which should have been allowed by access control policy without having to use exception mechanisms. Rafae et al have proposed policy refinement for better privacy coverage against exception based access in a typical healthcare setup [16]. The policy refinement is based on feedback from audit logs and system still needs to differentiate between violations and rules for refinement. In our scheme the sensitive information is available to primary doctors only and they can further share medical information for referral or second opinion without using exception mechanisms. The sensitive information in this case must have stronger requirements for access and audit under exception mechanisms than normal information.

Extensible Access Control Markup Language (XACML) is a policy specification language prepared by OASIS which allows access control policy formulation in XML. Policies are specified as set of rules and are created at Policy Administration Point (PAP). XACML also defines algorithms for combination of rules and policies to have deny-override, permit-override, first-applicable and only-one-applicable decisions. Access to resources is controlled by Policy Enforcement Point (PEP). When a user requests access to information PEP sends request to Policy Decision Point (PDP). The PDP then checks all applicable policies and determines whether permission should be granted. The response is then sent by PDP for enforcement to PEP which allows or denies access. Obligations are the operations specified in policy which must be performed by PEP along with authorization decision [17]. XACML profile of core and hierarchical RBAC have been developed but it still lacks separation of duty constraints of RBAC [18]. Temporal constraints like access from 9 AM to 5 PM interval or for duration of five hours can be specified in XACML [19] but it is not as expressive as temporal constraints in GTRBAC which allows specifying periodic constraints and also allows constraints for days of the week like 9 AM to 5 PM for Monday to Friday only.

3.1 Discretionary Access Control (DAC)

DAC is an access control mechanism that allows users to own objects or files and they can give permission to other users for objects under their control [20]. A strict DAC policy requires that owner is the only one who can grant access to an object and ownership cannot be transferred. A liberal DAC policy assumes that ownership can be transferred to other users based on single level grant or multi level grant [21]. DAC allows defining permissions for individual users on specific medical records. But the problem with DAC arises as the number of records and users grow, the updating of permissions is not scalable.

3.2 Role Based Access Control (RBAC)

Role Based Access Control (RBAC) has emerged as a standard for specifying permissions for a large group of users. It allows defining roles similar to the functional responsibilities of users in an organization and then giving permissions to roles [22]. RBAC policy consists of user, roles the user can assume and permissions available to each role. If a user assumes a role he gets all the permissions associated with that role.

Using contextual constraints like time and locations in RBAC we can restrict access to sensitive data of patients to users only during the authorized time and place. Generalized Temporal RBAC defines temporal constraints for RBAC using periodicity and duration constraints. The periodicity constraints can be used to specify the exact intervals for a role enabling and role assignment or permission assignment. While the duration constraints allow specifying durations for which enabling or assignment of a role and permission assignment is valid [23]. GTRBAC allows defining roles like night nurse or day physician which helps to ensure that the users have access to sensitive data only during the time shift they are working.

3.3 Policy Machine (PM)

Policy Machine (PM), developed by National Institute of Standards and Technology (NIST), provides the ability to configure and enforce arbitrary attribute-based access control policies [24]. It can enforce policies such as RBAC, DAC, Mandatory Access Control (MAC) and also combination of multiple policies. It helps to protect objects under one or more policy instances while enforcing these policies through a series of fixed PM functions that are invoked in response to user or subject access requests. User attribute (UA) is defined as mapping of user (U) to defined set of capabilities and U→UA is an assignment relation which means that user U has the properties denoted by attribute UA. Capabilities of a UA are derived from assignment of user attribute to operation set, where operation set is a set of operations. PM allows enforcement of multiple policies so that an object under two or more policies can only be accessed by a user if he can meet access control requirements for all applicable policies.

PM is a generalized access control mechanism and there can be different choices for its architecture and implementation. Reference implementation of PM is a three layer application consisting of Presentation layer, Application Logic layer and Data layer. The data layer uses MS Active Directory (AD) as a data repository and Lightweight Directory Access Protocol (LDAP) server as access mechanism. The application logic layer contains Policy Server which manages all data and relations stored in AD. The policy server provides services to admin client and session simulator. The admin client, session simulator, session manager, user sessions and user applications are part of presentation layer [21]. The policy to be implemented is specified in *.pm file which is loaded into AD by admin client. The admin client reads the policy specifications and sends them to policy server as commands. The policy server after parsing the commands loads permissions in appropriate containers of AD. The Virtual Object System (VOS) computation allows finding the objects accessible to a user attribute. During subject attribute activation the attributes are activated for users according to the capability. Finally reference mediation function grants permission if available.

4. Need for Multiple Policies against Insider Threat

Healthcare data contains information about patients ranging from regular hospital visits to sensitive information which the patient will like to keep as private as possible. The hospital information systems should have authorization mechanisms in place so that sensitive data of the patients is only available to primary doctor. A simple hypothetical scenario is considered to compare issues with different access control mechanisms for implementation of this requirement, where Alice and Bob are two doctors and A, B, C and D are four patients. All patients have declared some data as sensitive which should be available to the patient and primary doctor only. The primary doctor for A and B is Alice while for C and D it is Bob. Both Alice and Bob should be able to see the normal medical records for all patients and the patient can see all his medical records. The primary doctor may seek consultation on some sensitive record from other doctor. Now it is discussed how DAC and RBAC can be used to satisfy this requirement and what are the issues and how combination of policies can help to resolve these issues?

The use of DAC policy as authorization mechanism will require that both Alice and Bob are given access to all normal medical records of patients and for sensitive records only the primary doctor is given access as shown in Figure 2(a). But this scheme requires constant updating of access control lists as new CDA documents are created or new patients are added. The approach is not be scalable if we consider a large volume of CDA notes (50,000/week for Mayo clinic [6]) and the need to update access control lists of all doctors, support and admin staff.

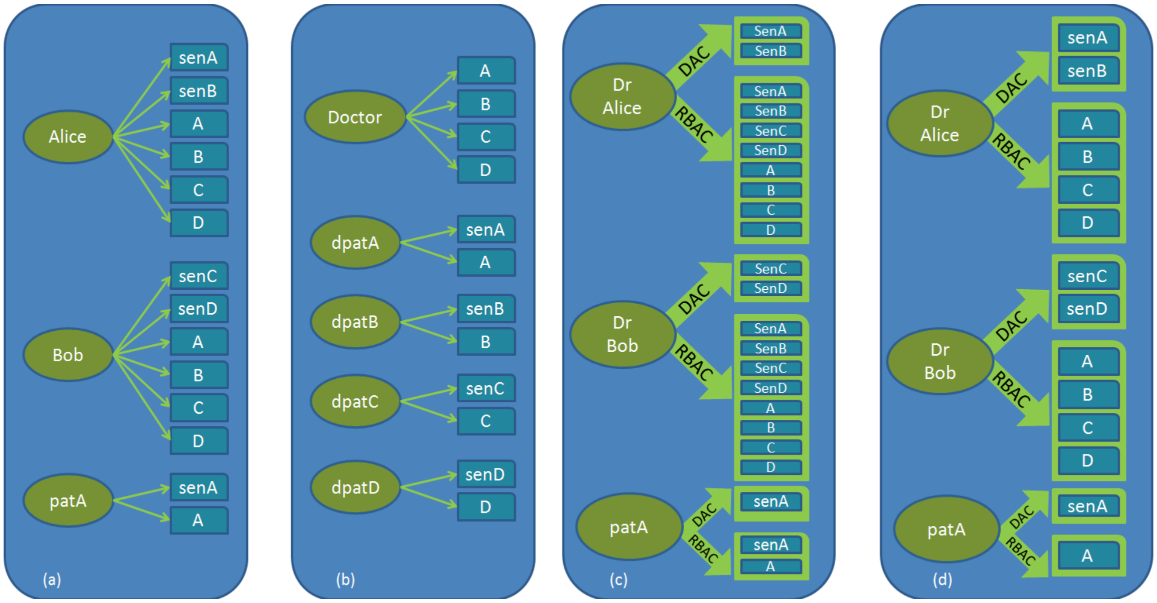


Figure 2. Comparison of Policies (a) DAC (b) RBAC (c) Sen in RBAC and DAC (d) Sen in DAC

RBAC allows to group users under one role and if the permissions are updated for a group these are valid for all users in that role. Using RBAC both Alice and Bob can take role Doctor and can access normal documents for all patients as shown in Figure 2(b). Each patient will need a unique role to access his own medical records (Role dpatA for accessing sensitive records of patient A). The sensitive information for a patient is also available under the same role and the primary doctor can access sensitive documents using this role. But still there are issues with consultation as this role cannot be shared with Bob. For consultation the primary doctor may need opinion on a single clinical document only but giving the role dpatA to consultant will give permission for all sensitive documents of patient A.

This problem can be solved by adding more roles to have unique roles for each doctor using which the sensitive information is made available to Alice and Bob for their own patients (Role senAlice for accessing sensitive records of Alice's patients). But still in case of consultation the doctor cannot share the roles. Another approach can be for example if Alice needs to consult Bob on some clinical note of patient A, she may ask the administrator to assign permission for that document to sensitive role of Bob as she under RBAC doesn't have the privilege for permission assignment. Here having sensitive information under DAC offers the benefit that patient or primary doctor owns the documents and can share them for second opinion or consultation.

Policy Machine is an attribute based access control mechanism which allows enforcement of multiple policies to give security policies which are scalable, context aware and allow discretionary access. PM allows flexibility in composing policies for healthcare and we can meet the requirements of having restricted access to sensitive records and usability by combining both DAC and RBAC in PM as shown in Figure 2(c) and 2(d). The policies can be defined such that the sensitive documents are in multiple polices as shown in Figure 2(c) in which user has to satisfy access requirements for both policies. This scenario corresponds to Figure 3(a) and the combination of policies allows us to use temporal features of GTRBAC and selective permissions of DAC. The medical records of all patients including sensitive records are available in RBAC to different roles. The sensitive records for a specific patient are assigned in DAC policy to the primary doctor. Now during reference mediation PM allows access to only those records for which users have permission in all applicable policies. A person can access sensitive medical record only if he has permission in both DAC and RBAC policy. The primary doctor can give access on a specific record for consultation and only this record will be available under DAC policy to the other doctor. Alice under PM has attribute doctor in RBAC by which she can access all records of all patients and attribute Alicia in DAC by which she can access sensitive records of A and B but she cannot access sensitive records of C and D for which she doesn't have permission in DAC. This combination gives the benefit that if a user cannot take a role in RBAC then even if he has discretionary access for a sensitive record the permission to access the records will be denied.

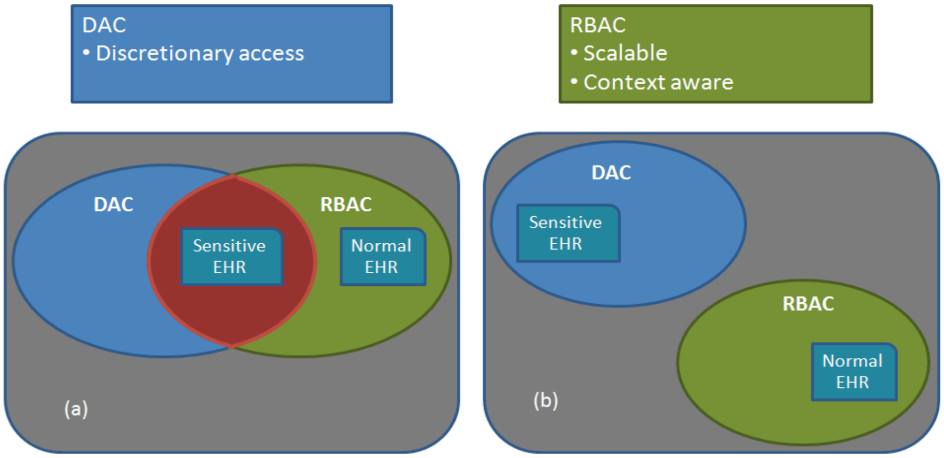


Figure 3. Permission set (a) Sen in RBAC and DAC (b) Sen in DAC

The combination by assigning sensitive records to both policies will cause limitations in some cases. For example we may need to use PM as in 2(d) when some sensitive information has to be shared with some other facility users of which are not part of any role in RBAC. Now having the sensitive information just under DAC allows use in internal facility as well as sharing of information with the external facility. The disadvantage of this approach is that as RBAC and DAC are mutually exclusive and the context aware features of RBAC cannot be combined with DAC as shown in Figure 3(b).

5. Security Policy for Healthcare

The basic design of access control for healthcare based on PM is shown in Figure 4. Here access of users to healthcare records is controlled by PM. Different types of clinical data may have different security policies and multiple policies can be enforced on a single document according to the requirement. A user request to access any Clinical Document (CD) is evaluated by PM by checking the status of user under a policy and available permissions to CD's are displayed to user. Principle of least privilege is implemented by restricting the permission set for roles by moving sensitive information under DAC policy where it is only available on "need to know" basis. The doctor treating the patient has access under DAC policy and the doctor might give access to a consultant on a specific document for opinion.

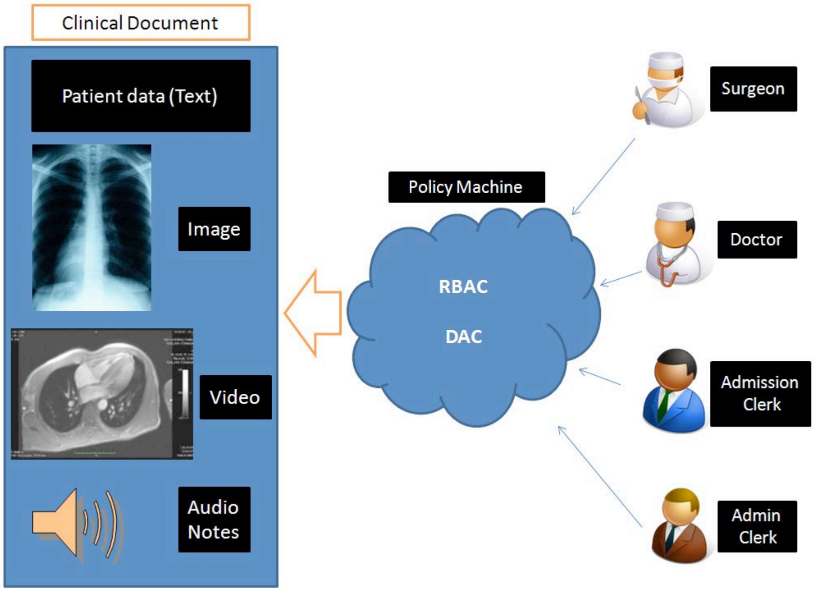


Figure 4. Multimedia Objects in a Clinical Document

A clinical document may contain images, videos or audio notes as shown in Figure 4. The multimedia objects which are part of a clinical document may have different permissions. For example a doctor may be able to see the radiology note under RBAC but not the X-ray image (if declared sensitive) which under DAC policy is only available to the surgeon treating the patient. The radiology note is displayed to the doctor without X-ray image and to the surgeon with image.

The PM architecture has been extended to add temporal context to RBAC so that time sensitive policies can also be enforced and an application for healthcare has also been added. The new architecture for healthcare is shown in Figure 5. All the clinical documents and their related multimedia content are stored in policy server. The user is logged in to session manager after authentication. The session simulator communicates with policy server and after VOS computation and subject attribute activation the relevant objects are displayed to user under applicable policies. The objects visible to a user in user-session can be accessed using CDA application developed for PM. The health records based on CDA are in XML format and the CDA application is launched whenever an XML object is accessed. The application reads the XML object and displays the clinical data and the associated multimedia content to user. The multimedia content is only displayed by CDA application if the user has permission to access them under some policy. CDA application currently developed and tested with PM is still a proof of concept and can display images and text in clinical documents. In future the functionality to play video and audio will also be added to the application.

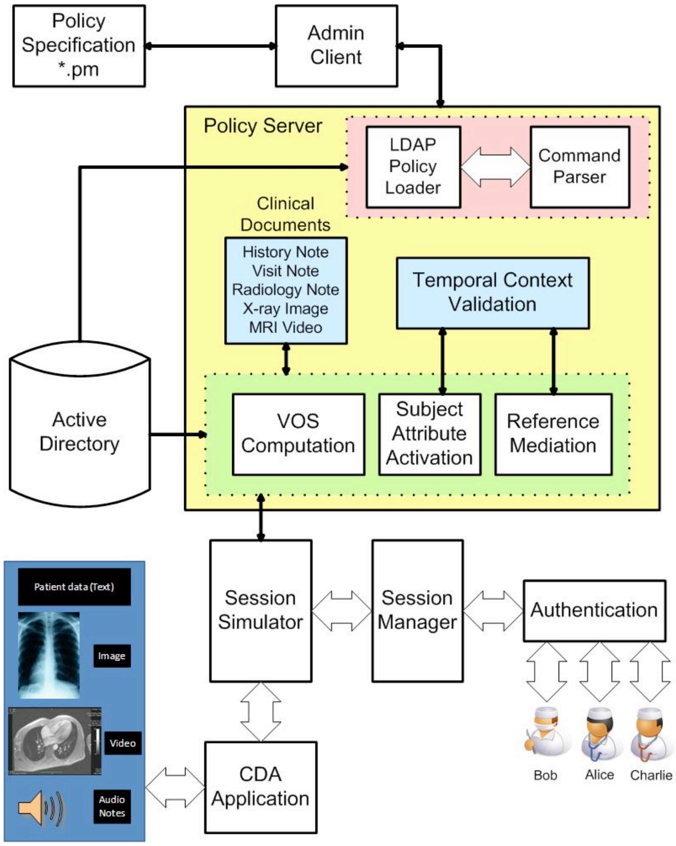


Figure 5. PM Architecture for Healthcare Application

6. Example Policy

An example policy is shown in Figure 6. The layout of policy is based on following rules.

- Any person in role doctor can see normal medical records of all patients but sensitive records are available for access to the doctor for his own patients only
- The role doctor may be active only during working days (Mon-Fri) from 9 am to 5 pm
- All patients can access their own medical records
- A doctor may allow access to a colleague to have consultation on some record for his own patients only

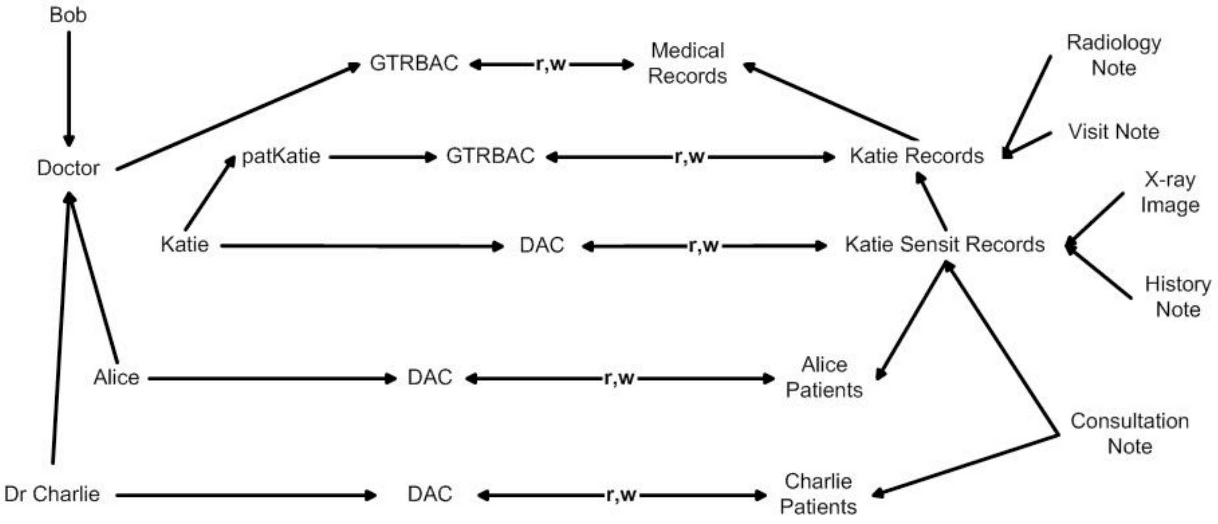


Figure 6. Example EHR policy on PM

The healthcare policy allows any person in role doctor to see normal medical records using GTRBAC but sensitive records are available for access to the doctor for his own patients only under DAC. The doctor may allow discretionary access to a colleague to have consultation on some record. We can see that Alice has access to sensitive objects under DAC policy and she can access all records of Katie under GTRBAC. But Bob has no access to sensitive records under DAC so he can only view normal records of Katie in role doctor. History note is controlled by two policies and Alice can only access it if she is active in role doctor in GTRBAC and with attribute Alicia in DAC. If for example the role doctor is not available to Alice after 5 pm then she will not able to access history note after 5 pm. Here although she has access under DAC policy but the permission is denied under GTRBAC policy after 5pm. In order to access an object under multiple policies, a user has to have permission for all applicable policies.

7. Conclusion

RBAC has been used for access control management for electronic health records. But a more stringent set of access control is required to prevent snooping and malicious use of sensitive data by users under a specific role. Access control for healthcare under PM allows assigning appropriate permissions under multiple policies like GTRBAC and DAC to control access to sensitive information. Users have to satisfy requirement of both policies which ensures that sensitive data is available only on need to know basis. Our contribution in this paper is to show that insider threat for healthcare can be mitigated by using access control mechanisms like DAC or RBAC but it comes with its own issues like scalability in DAC and the need to create multiple roles in RBAC. The policy machine can be used to solve both issues by using GTRBAC for normal records and DAC for sensitive records allowing benefits of both.

References

[1] European Court fines Finland for data breach, http://www.e-health-insider.com/News/3992/european_court_fines_finland_for_data_breach , 2009

[2] R. N. Charette, Dying for Data, *IEEE Spectrum*, Vol. 43, No. 10, October 2006, pp: 22-27

[3] More UCLA staff saw celebs' health records, http://www.usatoday.com/news/nation/2008-08-05-ucla-celebrity-records_N.htm, 2009

[4] Private health records not so private, http://abcnews.go.com/US/Story?id=3714207&page=1, 2009

[5] US Dept of Health and Human Services, Office of Civil Rights. Unofficial Version of HIPAA Administrative Simplification Regulation Text, 45 CFR Parts 160, 162, and 164, as amended through February 16, 2006. Available at http://www.hhs.gov/ocr/AdminSimpRegText.pdf

[6] R. H. Dolin, L. Alschuler, S. Boyer, C. Beebe, F. M. Behlen, P. V. Biron and A. Shabo: HL7 Clinical Document Architecture, Release 2. J*ournal of the American Medical Informatics Association*, Vol. 13, No. 1, 2006, pp: 30-39

[7] T.C. Rindfleisch, Privacy, information technology, and health care, *Communications of the ACM*, Vol. 40, No. 8, 1997, pp: 92-100

[8] R. Bhatti, A. Samuel, M. Y. Eltabakh, H. Amjad, and A. Ghafoor: Engineering a Policy-Based System for Federated Healthcare Databases, *IEEE Transactions on Knowledge and Data Engineering*, Vol. 19, No. 9, 2007, pp: 1288-1304

[9] R. Bhatti, A. Ghafoor, E. Bertino, and J. B. D. Joshi, "X-GTRBAC: An XML-based Policy Specification Framework and Architecture for Enterprise-wide Access Control", *ACM Transactions on Information and System Security*, Vol. 8, No. 2, May 2005, pp: 187–227

[10] A. Ferreira, R. Cruz-Correia, L. Antunes and D. Chadwick, Access Control: How Can It Improve Patients' Healthcare? , *Studies In Health Technology And Informatics,* Vol. 127, 2007

[11] B. Alhaqbani and C. Fidge, "Access Control Requirements for Processing Electronic Health Records", *Lecture Notes in Computer Science*, Vol. 4928, 2008, pp: 371-382

[12] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Hippocratic Databases," *in Proceedings of the 28th international conference on Very Large Data Bases*, 2002, pp: 143–154

[13] R. Agrawal, A. Kini, K. LeFevre, A. Wang, Y. Xu, and D. Zhou, "Managing Healthcare Data Hippocratically*," in Proceedings of the 2004 ACM SIGMOD international conference on Management of data*, 2004, pp: 947–948

[14] R. Agrawal and C. Johnson, "Securing Electronic Health Records without Impeding the Flow of Information," *International journal of medical informatics*, Vol. 76, No. 5-6, 2007, pp: 471–479

[15] L. Rostad and O. Edsberg, "A Study of Access Control Requirements for Healthcare Systems based on Audit Trails from Access Logs," *in Computer Security Applications Conference*, 2006, pp: 175–186

[16] R. Bhatti and T. Grandison, "Towards Improved Privacy Policy Coverage in Healthcare using Policy Refinement," *Lecture Notes in Computer Science*, Vol. 4721, 2007, p: 158

[17] T. Moses et al., "Extensible Access Control Markup Language (XACML) version 2.0,"*Oasis Standard*, Vol. 200502, 2005

[18] A. Anderson, "Core and Hierarchical Role Based Access Control (RBAC) Profile of XACML v2.0," *OASIS Standard*, 2005

[19] W3Schools, "XSD date and time data types." http://www.w3schools.com/Schema/schema dtypes date.asp, 2009

[20] N. C. S. Center, "A Guide to Understanding Discretionary Access Control in Trusted Systems," *NCSC-TG-003-87*, 1987

[21] S. I. Gavrila, "The Policy Machine Architecture, Data Structures, Algorithms, and Configuration", *NIST Internal Document*, September 19, 2007

[22] D. F. Ferraiolo, R. Sandhu, S. I. Gavrila, V. C. Hu, D. R. Kuhn and R. Chandramouli, “Proposed NIST standard for role-based access control”, *ACM Transactions on Information and System Security (TISSEC)*,Vol. 4, No. 3, 2001,pp: 224-274

[23] J.B.D. Joshi, E. Bertino, U. Latif and A. Ghafoor, A Generalized Temporal Role-Based Access Control Model, *IEEE Transaction on Knowledge and Data Engineering*, Vol. 17, No. 1, 2005, pp: 4-23

[24] D. F. Ferraiolo, S. I. Gavrila, V. C. Hu and D. R. Kuhn, “Composing and Combining Policies under the Policy Machine”, In Proceedings of the *Tenth ACM Symposium on Access Control Models and Technologies*, June 2005,pp: 11-20