A Survey on Different Type of Access Control Model for Personal Health Record (PHR) System

Sapna Patel[1], G.J. Sahani[2]

[1]M. E. Student, Dept. of Computer Engineering, Sardar Vallabhbhai Patel Institute of Technology, Baroda, India

[2]Asst. Prof., Dept. of Computer Engineering, Sardar Vallabhbhai Patel Institute of Technology, Baroda, India

***Abstract*—Access control is a mechanism by which protect the information assets of the enterprise from unauthorized access. Access control is one of the feature to provide security which help other system. Now a days, healthcare systems are is becoming popular. To improve access model in healthcare there are many research has taken place. In this paper described the different ways of access model for removing the privacy and security issue in healthcare.**

***Index Terms*—DAC, MAC, RBAC, ABAC, PHR**

I. Introduction

The objectives of an access control system are often described in terms of protecting system resources against inappropriate or undesired user access. From a business perspective, this objective could just as well be described in terms of the optimal sharing of information. After all, the main objective of IT is to make information available to users and applications. A greater degree of sharing may get in the way of resource protection; in reality, a well-managed and effective access control system actually facilitates sharing. A sufficiently fine-grained access control mechanism can enable selective sharing of information where in its absence, sharing may be considered too risky altogether.

When planning an access control system, three abstractions of controls should be considered: access control policies, models, and mechanisms. Access control policies are high-level requirements that specify how access is managed and who, under what circumstances, may access what information. While access control policies can be application-specific and thus taken into consideration by the application vendor, policies are just as likely to pertain to user actions within the context of an organizational unit or across organizational boundaries.

Access control policies are enforced through a mechanism that translates a user's access request, often in terms of a structure that a system provides. There are a wide variety of structures; for example, a simple table lookup can be performed to grant or deny.

Rather than attempting to evaluate and analyze access control systems exclusively at the mechanism level, security models are usually written to describe the security properties of an access control system. A model is a formal presentation of the security policy enforced by the system and is useful for proving theoretical limitations of a system. [1]

In recent years, personal health records (PHR) online has become more popular. A number of providers have started providing services, which allow patients' health data to be used more easily, such as the Microsoft HealthVault [2], Google Health [3] and WebMD [4].

According to HIPAA(Health Insurance Portability and Accountability Act) provide rule and regulation regarding generation of healthcare system .The number of electronic health records (EHRs) is expected to grow even larger in the coming years as more facilities adopt electronic records, and rely increasingly on mobile applications and devices such as tablets and smartphones to gather this patient information [5].1 In Australia, the Government has recently announced an EHR system called the personally controlled electronic health record (PCEHR) system [6] to assist patients in better organizing their PHR and provide the patients with flexibility in controlling the access to their PHR.

II. Literature Review

There are different kind of access control like DAC, MAC, RBAC, ABAC .

Deborah D.et al [7] In DAC 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. 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. Verifying the correctness of the DAC mechanism is difficult.

Yanfang Fan, et al [8] MAC has better security than DAC, since it can control indirect information flows. Access to system resources are safe guard using Security levels shared between User and System Administrator. Flexibility is a key problem when system with MAC is put into effect. Classical BLP model contains DAC but can't really embody its advantage of flexibility. FEMAC model integrates the MAC with DAC. Not only has the security of MAC but also has the flexibility of DAC. Through introducing special security property, temporary authorization is adopted to improve flexibility further. FEMAC is not a simple "and" or "or" relation of DAC and MAC. It's a real integration of two kinds of access control modes. It considers the relationships between these two access control modes. We analyze the possible information flows between two kinds of access control modes and assure they are legal in FEMAC.

D. F. Ferraiolo et. al. [9] given paper important content related:

1) Core RBAC
2) Hierarchal RBAC
3) Constrained RBAC

Core RBAC have simple structure having user-role and permission-role assignment can be many-to-many.It also have e concept of user sessions, which allows selective activation and deactivation of roles.

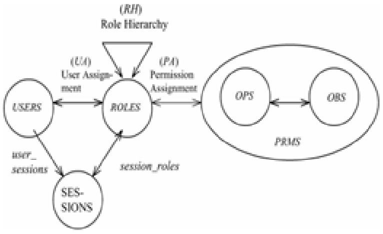

Fig. 1. Hierarchical RBAC

Hierarchical RBAC is partial order defining a seniority relation between roles, whereby senior roles acquire the permissions of their juniors, and junior roles acquire the user membership of their seniors. This standard recognizes two types of role hierarchies: 1) General Hierarchical RBAC. 2) Limited Hierarchical RBAC.

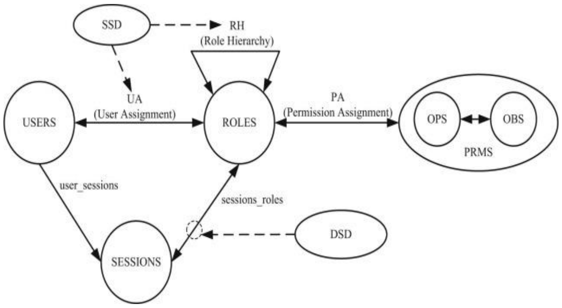

Fig. 2. RBAC with SSD and DSD

Constrained RBAC adds separation of duty relations to the RBAC model. SSD is role based system may arise as a result of a user gaining authorization for permissions associated with conflicting roles Membership in one role may prevent the user from being a member of one or more other roles,. DSD (Dynamic Separation of Duty Relations) limit the availability of the permissions by placing constraints on the roles that can be activated within or across a user's sessions.

Vincent C. Hu et, al. [10] Access control or authorization, on the other hand, is the decision (implicit or explicit) to permit or deny a subject access to a specific object (network, data, application, service, etc.) The terms access control and authorization are used synonymously throughout this document. The policy is used to convey these rules and relationships. Policy is typically written from the perspective of the object that needs protecting and the privileges available to subjects. OASIS XACML specification by providing a basic definition, concepts, and components that make up an ABAC model policies are written in it.The access control mechanism often employs a policy decision point (PDP) to render a decision, a policy enforcement point (PEP) to enforce the decision, and some sort of context handler or workflow coordinator to manage the collection of attributes required for the decision.

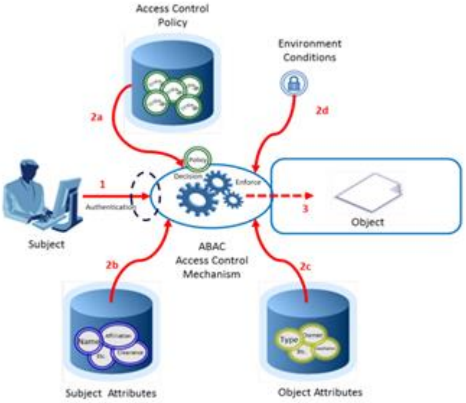

Fig. 3. Basic ABAC access control scenario

Rose Ann S. et, al. [11] discover the Task-Role-Based Access Control (TRBAC) is an access control model developed to put constraints on the tasks and the corresponding roles of those who will try to access a system. The user with assigned role or roles would activate some of those roles through a session. Tasks are assigned to users via their role/roles in the system. A user's permission to access certain files is determined by the tasks assigned to him. Constraints are important aspect of access control and are a powerful mechanism for laying out higher-level organization policy. With constraints, we would be able to address some issues that RBAC and TBAC models left open .In this paper they have taken scenario of healthcare. The following a constraints are added for role constraint 1) Mutually Exclusive Roles 2) Role Hierarchy 3)Privilege Constraint 4)Prerequisite Role 5)Interval and Duration and for task constraint 1)Least Privilege2)Task Priority3) Start Time4) End Time as shown in Fig. 4.

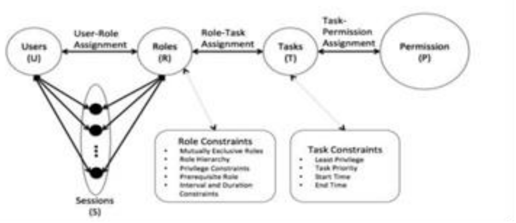

Fig. 4. Task - Role based access control model

Xin Jin1 et al [12] propose a first model that integrate roles and attributes using the role centric methodology. This model extends the RBAC model with permission filtering policy. They use PFP to find out the available set of permission which contained user and object attribute as shown in Fig. 5.

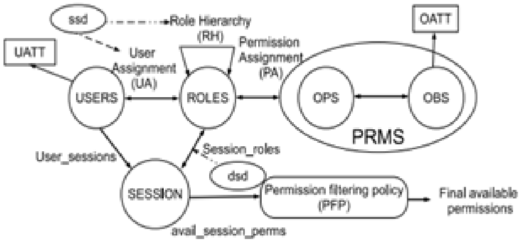

Fig. 5. RABAC model

In Fig. 6, the maximum permission set available in a session is represented by the available session permission function. Filtering policy provide the constrained on these available permission set. There is set of filter function {F_1, F_2, F_3…..F_n} for the purpose of providing a constraint. Each filter function is a Boolean expression contained user and object attribute. There is a Target Filter function that maps each data object to a subset of this filter functions. This mapping is based on the attributes expression which contained the object attribute called a condition which is used to determine whether each filter function is applicable or not. The applicable filter functions are invoked one by one for each of the permissions in available session permission. If any of the functions return FALSE, the permission is blocked and removed from the available permission set for this session. And At the end of this process, we get the final available permission.

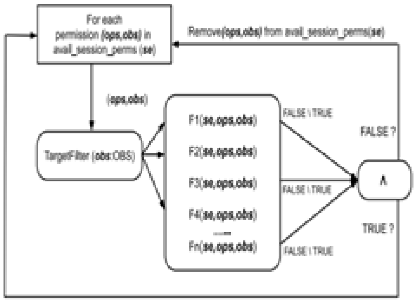

Fig. 6. Permission filtering process

Jingwei Huang et al [13] developed a model in two levels 1) aboveground 2) underground. The aboveground level is simple and standard RBAC model extend they use the attribute based policy to explicitly represent RBAC modelled with environmental constraint. In underground level, hence creating RBAC model in aboveground. They use ABAC policy to automatically assign user to role and role to permission as shown in Fig. 5. The model provide fine grained access control but using large number of role hence there is role explosion problem and it is somewhat complex because for user to role and role to permission assignment they have to define the attribute based policy.

They also consider the environmental condition so it is context aware .Auditing and policy visualization is difficult because role is assigned to user based on policy so that role can be change on changing policy and it is not clear that what set of user will be effected by changing in policy.

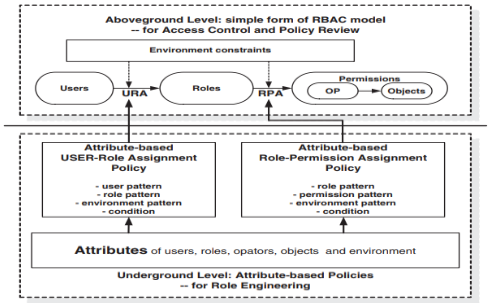

Fig. 7. . A two-layered framework integrating attribute-based policies into RBAC

Hui Qi et al [14] propose a model in which they preserve the full RBAC model. They use the ABAC as a constraint on user to role assignment and role to permission assignment. They dynamically adjusting the role that the user is associated with and the permission that the role is associated with by attribute based access control rules. The new model can be expressed as:

$$U \xrightarrow{A1,\ldots\ldots, An} R \xrightarrow{A'1,\ldots\ldots, A'm} P \qquad (1)$$

Ai and Aj in (l) are the constraint attributes of U –> R and R -> P respectively. They are not directly involved in U - > Rand R - > P mappings. Instead, they are used to filter the association relationships after the establishment of U - > R and R - > P mappings. As shown in Fig. 1, ABAC is used as constraint on user to role assignment and role to permission assignment.

Since full RBAC model is preserved it is simple to manage and Audit. It also provides fine grained access control because all dynamic and static attribute is considered during access control. The model is context aware because during role to permission assignment they taken the dynamic attribute such as time, location etc. in to account. Multi domain implementation of this model is somewhat difficult because first it is based on RBAC model second attribute.

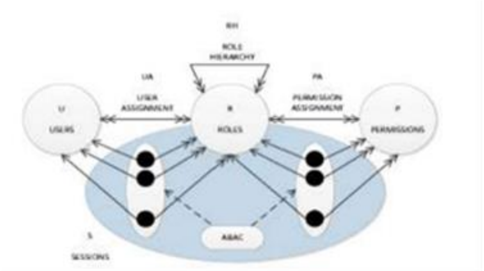

Fig. 8. RBAC-ABAC model

Under as constrained during user to role and role to permission mapping May different in different domain that makes the filtering of user to role and role to permission assignment a difficult task. This model solves role explosion of RBAC and the access control rule explosion of ABAC. For example, if there are n attributes in the system, RBAC and ABAC will respectively generate 2^n roles and 2^n access control rules, while the new model will divide n attributes into x static attributes and n - x dynamic attributes, and then sets up 2^x roles for x static attributes and sets up 2^n-x access control rules for n - x dynamic attributes, so that the total will be reduced to 2^x + 2^n-x.but if no. of static attribute and no. of dynamic attribute is more than no. of role and rule is again increases hence there is still a problem of role and rule explosion.

Lawrence Kerr et. al [15] represents a combined MAC and ABAC model. They take the classification, clearance and compartment of the MAC model as mandatory attribute in ABAC model. By taking classification, clearance and compartment as mandatory attribute they combine the traditional MAC model in ABAC model while preserving the flexibility of ABAC model. The classification of objects or clearance of subjects, as well as compartments is treated as attributes. This model has all the advantages of ABAC such as fine grained, context aware as well maintaining the basic principles of a MAC model. Since it also suffer from the limitation of ABAC such as difficult to audit, hard to visualize the policy modification.

Qasim Mahmood Rajpoot et al [16] in their approach provides fine-grained access control mechanism that not only suitable for applications where access to resources is controlled by contents of the resources in the policy but it also takes contextual information into account while making the access control decisions. Their solution has the following key features: a) it allows to make context-aware access control decisions by associating conditions with permissions that are used to verify whether the required contextual information holds or not when a decision is made, b) it offers a content-based authorization system while keeping the approach role-oriented, in order to retain the advantages offered by RBAC. They achieve this by allowing specifying permissions using attributes of the objects rather than using only identifier. The entities in figure 6 such as users, roles, objects and operations have the same semantics as in RBAC. Users and objects in this model are associated with attributes too. They also incorporate the environment attribute to support the situation where contextual attribute are required in access control decision. The dotted-box in Figure 6 represents the modules of the architectural design to enforce this model.

Using the proposed approach, they provide fine-grained access control mechanism without creating a large number of roles. The model is context aware because it takes environmental condition while performing access control. It simpler to audit what permissions may be granted to a user because of being role-centric. It is relatively easy to visualize what the impact of adding is or removing a policy since policy specification is at the level of role. Therefore, a change in policy can affect only those users who are assigned to a role being modified.

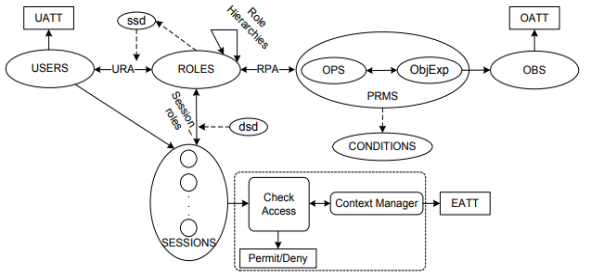

Fig. 9. A two-layered framework integrating attribute-based policies into RBAC

III. Comparison between Techniques

All the above research paper has been compared on the basis of the functionality like fine grained, context aware, auditing and role explosion. This functionality described below: [16]

Fine-grained Access Control: RBAC provides a coarse-grained access control model where as many applications require a much Finer-degree of granularity.

Context-aware Access: RBAC cannot easily handle dynamically changing attributes. It typically does not support making contextual decisions unless many similar roles are created causing role-explosion problem. We provide a mechanism to incorporate these dynamically changing attributes in a role-centric manner yet without requiring to create a large number of roles. Example of context aware access is location, time etc

Auditing: Auditing is simple in RBAC system rather than ABAC .When ABAC is used in a considerably large organization having a large number of policy rules, it may not be practically feasible to audit what permissions have been granted to a user. In ABAC, any combination of attributes may essentially grant an access and hence it requires to analyze all policy rules with an exhaustive enumeration of attributes used in each policy rule

Role explosion: In RBAC Role explosion problem. Because there is no concept of role instead there is centralized policy. In

TABLE I
COMPARISON OF PAPERS

Paper	Feature			
	Fine grained	**Context aware**	**Auditing**	**Role explosion**
Deborah D.et al [7]	No	No	Not possible	There is no role
Yanfang Fan, et al [8]	No	No	Not possible	There is no role
D. F. Ferraiolo et al.[9]	No	No	Not possible	Yes
Vincent C. Hu et, al. [10]	Yes	Yes	Easy	No
Rose Ann S et, al. [11]	No	No	Easy	No
Xin Jin1 et al [12]	No	No	Easy	No
Jingwei Huang et al [13]	Yes	Yes	Difficult	Yes
Hui Qi et al [14]	Yes	Yes	Easy	Yes
Lawrence Kerr et al [15]	Yes	Yes	Difficult	-
Qasim Mahmood Rajpoot et al [16]	Yes	Yes	Easy	No

ABAC there is role explosion problem because we have to define so many role in order to provide fine grained access.

Access control is used to restrict the unauthorized user and in RBAC access control system the access of object is provided on the basis of role .particular role is allocated to the object. Role are given priority .ABAC access control is basically based on giving access on the basis of environmental attribute like location, time etc. which is more flexible than other access control . This both access control was famous till now they both have some advantage and disadvantage .So access system have made which will integrated the advantage of both system and remove disadvantage and some are successful to such extend. The integration of ABAC and RBAC is a revolution in the access control system. There are more access system like MAC, DAC etc. I have given the difference in the system of some research paper on the basis of above functionality in Table-I.

IV. CONCLUSION

Access control is used to stop the unauthorized user to access object. There is different types of access control ABAC and RBAC and many more but this two are most famous and reliable among other access control. This paper have comparison of access control on the basis of fine grained, context aware, auditing, role explosion.

REFERENCES

[1] Vincent C. Hu David F. Ferraiolo D. Rick Kuhn ”Assesement of access control system” ,NIST U.S. Department of Commerce, Sep,2016
[2] Microsoft, Microsoft healthvault. https://www.healthvault. com/
[3] Google. Google health. http://www.google.com/health
[4] Webmd. http://www.webmd.com/.
[5] Savaiano, J. (2014) Managing the healthcare information stream. http://webdocs.commvault.com/assets/2014-healthcare-survey. pdf.
[6] Government, A.F. (2012) Personally controlled electronic health record system (pcehr) document. http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/ pcehr-document.
[7] Deborah D. Downs, Jerzy R. Rub, Kenneth C. Kung, Carole S, Jordan, “Issues in Discretionary Access Control”, Security and Privacy, IEEE, , April 1985.
[8] 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, Nov 2009.
[9] David F. Ferraiolo , Ravi Sandhu, Serban Gavrila, D. Richard Kuhn and Ramaswamy Chandramouli,” Proposed NIST Standard for Role-Based Access Control”, ACM Transactions on Information and System Security, Vol. 4, No. 3, August 2001, Pages 224–274
[10] Vincent C. Hu ,David Ferraiolo and Rick Kuhn,” Guide to Attribute Based Access Control (ABAC) Definition and Considerations (Draft)”, NIST Special Publication 800-162,April 2013
[11] Rose Ann S. Zuniga1 and Susan P. Festin ” A Design for Task-Role Based Access Control for Personal Health Record Systems”, Philippine Engineering Journal PEJ 2017; Vol. 38, No. 1: 27-38.
[12] Xin Jin, Ravi Sandhu, and Ram Krishnan” RABAC: Role-Centric Attribute-Based Access Control” Springer-Verlag Berlin Heidelberg 2012
[13] Jingwei Huang, David M. Nicol, Rakesh Bobba and Jun Ho Huh” A Framework Integrating Attribute-based Policies into Role-Based Access Control” SACMAT'12, June 20–22, 2012.
[14] Hui Qi, Hongxin Mat, Jinqing Li and Xiaoqiang Di ” Access Control Model Based on Role and Attribute and its Applications on Space-Ground IntegrationNetworks” IEEE 2015.
[15] Lawrence Kerr, Jim Alves-Foss “Combining Mandatory and Attribute-based Access Control” IEEE 2016.
[16] Qasim Mahmood Rajpoot, Christian Damsgaard Jensen and Ram Krishnan” Attributes Enhanced Role-Based Access Control Model” Proceedings of the 12th International Conference on Trust, Privacy and Security in Digital Business (TrustBus’15). (pp. 3-17). Springer.