International Journal of Engineering & Technology, 7 (2.8) (2018) 554-558

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Evolution of access control models for protection of patient details: a survey

Geetanjali Sinha[1*], Prabhu Shankar K.C[2], Shaurya Jain[3]

[2]Assistant Professor, Department of Computer Science and Engineering,
[1,3]Students, Department of Computer Science and Engineering, SRM University, Chennai, Tamil Nadu, India
**Corresponding Author E-mail: geetanjali1202@hotmail.com*

Abstract

Hospitals across the world are adapting to Electronic Hospital Information Systems and are moving away from the manual paper systems to provide patients efficient services. Numerous Access Control Models have been deployed for securing patient privacy one of them being Role Based Access Control Model (RBAC). The current models merely allow access on the basis of roles and role hierarchy without actually understanding the real intention of the person accessing the system. This could lead to a compromise of patient privacy and thus new methods have been evolving. In this survey we will see an evolution of the access control models which lead to the discovery of KC-RBAC (Knowledge Constrained Role Based Access Control) Model which takes into consideration the knowledge related to the medical domain along with the role to provide authorization.

Index Terms: *Access Control Models, DAC, Hospital Information System, MAC, KC-RBAC, RBAC, Patient Privacy*

1. Introduction

In the present times factors which are of utmost importance are technology and information [1]. Everything is now being stored online or in electronic mediums and databases to make work more efficient and services user friendly. Many organizations are shifting to electronic storages of data like banks and Hospital Information Systems.

But every good thing comes with a flaw. The flaw here is security. Due to the wide availability of data anyone from anywhere can access data which he is not supposed to putting at risk the personal information contained in the data.

Thus it became necessary to adopt security measures for protection of data and maintenance of privacy.

One of the methods adopted was the use of Access Control Models. Several organizations have started using the access control models which provide authorization on the basis of role, knowledge, etc. All work with the main aim to mitigate unauthorized access to system data and resources.

This surveystudies the use of various access control models and their evolution for a Hospital Information System for the provision of patient privacy

The paper is further divided into the following sections:

Section II describes what is a Hospital Information System and why is privacy needed. Section III describes the evolution of the various Access Control Models and their use in security. Section IV describes the various modifications that have been made to RBAC for better privacy. Section V describes the migration of RBAC to KC-RBAC. Section VI gives an overview of KC-RBAC is and finally we conclude the paper with Section VII.

2. Hospital Information System

Hospital Information System (HIS) is a highly exclusive application which is developed by the management who use computers and technology in a hospital [2]. A fully digital hospital

works with the aim of integrating applications of information technology, communications, computer science algorithms and evolve from the traditional mode of operation that is maintaining all records manually on paper. This method would help achieve better disease prevention and health care treatment [3]. Electronic paper based records have changed the face of healthcare.

A Hospital Information System basically contains of patient details and it has a number of sources. It contains information about the disease a patient encountered , which doctor treated him , what treatment was given, what was the mode of payment, what medicines were administered, etc. Some of this data can be shared but otherwise all other data should remain private for the benefit of the patient [4].

Fig. 1: Components of a Hospital Information System

The importance of protection of patient details is of prime importance. HIS contain sensitive information which if not handled with care can become a target of malicious and unauthorized access which may cause serious violation of personal privacy and open doors to various other abuses. Due to the increase in these attacks on patient details it has become very important to protect their privacy [5].
There are many techniques that have been deployed to protect patient privacy. Some of these include encryption, data masking and the most famous one Access control Models.One of the most famous models in use is the RBAC model.

3. Evolution of Access Control Models

Over the passing time there have been many access control models that have been put to use.The requirements for managing the large databases of the banks or hospital systems are increasing and thus many access control models are coming to light.
But due to the varied sizes of the databases it becomes impossible to control the accesses. Therefore some researchers came up with the idea of combining all the different types of models and making the work as one [7].
Thus many techniques are being adapted like combining of different models or forming of new models while others are extensions of the already existing models.
A few of the important models were MAC, DAC and RBAC.

A. MAC

MAC stands for Mandatory Access Control. It was designed by Bell and LaPadula. It is also called as the Latices based Access Control which was designed as a better access control model than DAC [6].
In MAC there are two classifications namely the subject and the object. There are special security attributes that are allotted to the subject and object. A subject cannot change the attributes of another subject but according to the security attributes it has the right to access the particular objects.
According to the security rules, a subject can perform two functions namely read and record. It can read objects which are at its same level or levels lower than it and it can record objects which are at its level or level higher than it.[7].
Objects have classifications and subjects are entitled with clearance. Access control decisions are made based on the relationship between object classification and subject clearance [8].

MAC can also be categorized in the following two categories namely Multilevel and Multilateral Security.
MAC contains the flexibility. It provides security against Trojan horses as well. But one of the main problems with MAC was Data Integrity and also that it does not provide a dynamic environment. Also after its implementation MAC requires a lot of high system management and thus new models had to be searched for.

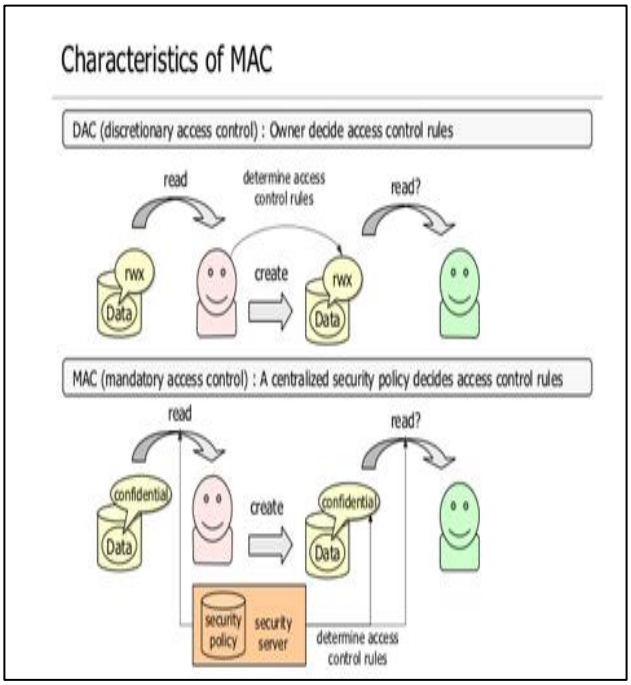


Fig. 2: Comparisons of MAC AND DAC

B. DAC

DAC stands for Discretionary Access Control. It is derived from the access matrix model. It restricts the access of the subject to an object on the basis of the subject's identity.
It works on the principle that a user can grant access to any object under him and the access control privileges are to be left to the discretion of the individual users.
DAC gives the user the freedom to revoke or grant the access to objects that belong to them. This can be considered as one of the major problems as it makes access control discrete.
Though it has more access flexibility than MAC it cannot control illegal flow of data to unauthorized user and once it has given the authorization it does not have any control over the flow of data. Due to its global policies DAC also has issues in maintain consistency. It can be prone to viruses as well. Also the identity of a subject in DAC is crucial because actions can get performed from another person's identity as in DAC a user can grant access right to another user and thus this a drawback of DAC as it can be prone to Trojan horses and malicious attacks [6][7][8][9].

C. RBAC

One of the most favourable access control models which has been deployed all over is the RBAC which stands for Role Based Access Control Model. RBAC consists of a set of components namely roles, permissions, users, sessions. RBAC controls the access to information based on the user activity.
It gives authorization to the user to access the information according to the roles the user performs. Roles can be defined as job functions of an organization and the roles are assigned to the user according to the organizational requirements [2][5][7]. It can be seen as a variation of the access matrix.

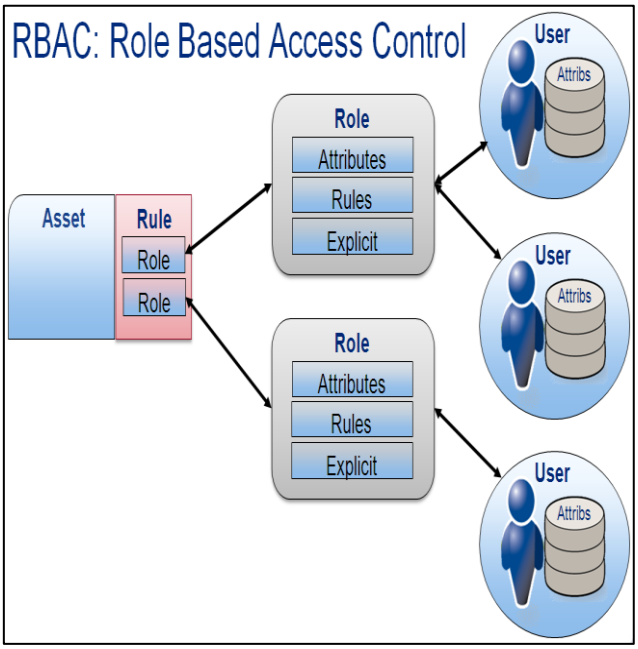


Fig. 3: Architecture of RBAC

It is important to maintain the hierarchical order between the roles in order to create the inheritance pattern between the roles. This is necessary to create the access rights in accordance to the hierarchical order of the role of the person in the organization and it helps in understanding whether that level has the right to access the data or not. The different forms of hierarchical RBAC's are RBAC1. RBAC3 combines the features of RBAC1 And RBAC2 [11].

There are many advantages of using RBAC like authorization management, provision of hierarchical role, separation of duties etc.

But all that glitters is not gold. Though RBAC can be least complex and most efficient model of implementation it has it flaws. RBAC cannot incorporate contextual constraints in it. RBAC does not provide fine grained results and it provides roles statically to the user which is not beneficial in a dynamic environment.

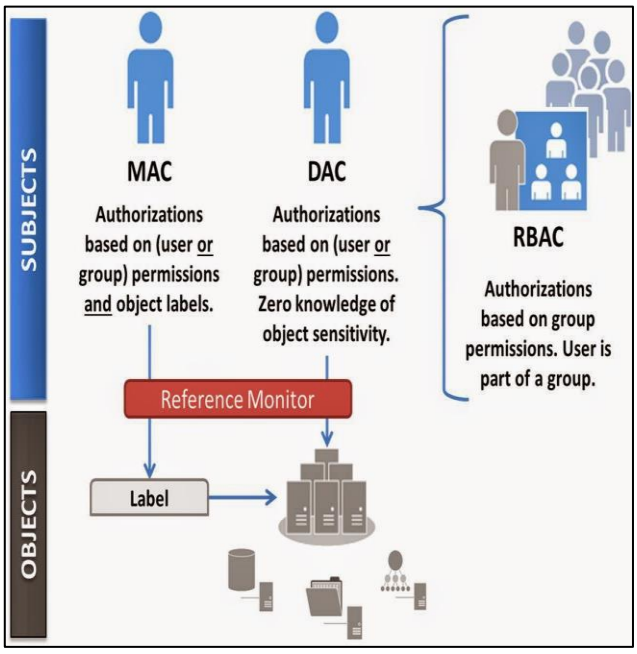


Fig. 4: Comparisons of RBAC, DAC and MAC

4. Modifications Made to RBAC and Work done on it

There have been many research works done to overcome the shortcomings of RBAC and many extensions have been performed on it. Some of these have been discussed in this section.

Researches conducted in 2012 proposed a system of combining RBAC along with DAC and context- aware access control system. RBAC takes the data from the web ontology and sees what roles should be generated in a medical system and DAC in extension with RBAC performs the function of tokenization and verification. Further in many researches ABAC was introduced as an extension to RBAC. RBAC has been condemned for its inflexibility and its static nature. These issues can be solved with the help of ABAC. ABAC stands for Attribute based access control model.

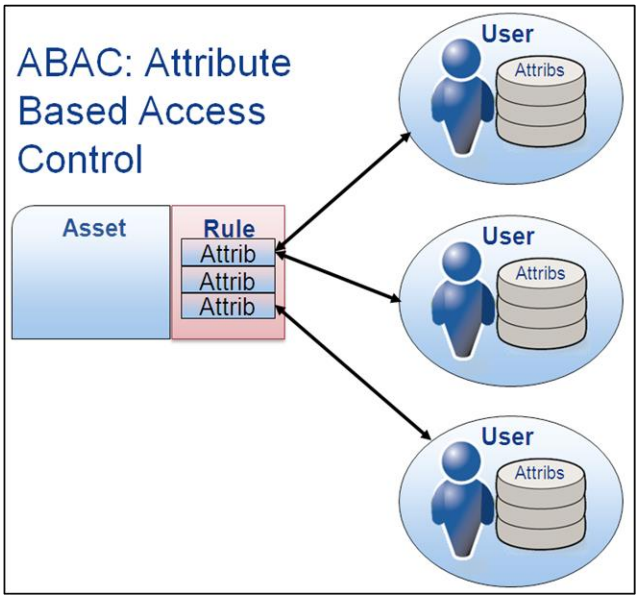


Fig. 5: Architecture of ABAC

ABAC supports RBAC by adding flexibility by the use of attributes for role determination instead of user identity. Since attributes are associated with both the resources and users, it allows dynamic specification of privileges for resources and association of users with privileges. Since ABAC is easily configured it is easy to implement it in dynamic environments. But because of its easy implementations there are some problems which are faced them being that changing or analyzing of permissions becomes complex [8]. Lawrence Kerr, Jim Alves-Foss also proposed a MAC and ABAC access control model. But again there were the shortcomings of ABAC being faced [8].

In another research by Min-A Jeong et.al decided to generate a model comprising of MAC, DAC and RBAC. It would function in two stages namely the first stage consisting of modified MAC (Mandatory Access Control) model and RBAC (Ro1e-Based Access Control) model. The user can access the data which is at the level which or at level lower to which his role can access. In the second stage a modified DAC model is applied to control the 'read' mode as it filters out the non-accessible data from the results obtained from the first stage. In this way the user can access the data that he is authorized to access [7].

Another migration observed was to TRBAC that is Temporal RBAC. Since RBAC does not include temporal, spatial or environmental constraint on the availability of roles to users a number of modifications and extensions have been proposed. Temporal RBAC restricts the time duration during which a role can be enabled.

But besides all these systems there were some problems which were still being faced.

The table below lists out some differences between the models:

Tab**le 1:** Comparison of different Models

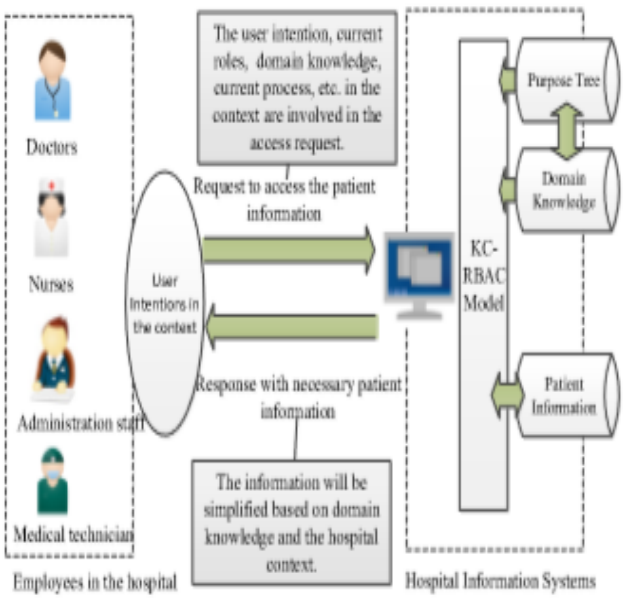
	RBAC	DAC	MAC	ABAC
METHOD	It works by segregating roles	It gives the rights to the users	It provides security clearances	It uses attributes to grant permissions
INTEGRITY	YES	NO	YES	YES
PRONE TO MALICIOUS ATTACKS	NO	YES	YES	NO
AUTHORIZATION MANAGEMENT	YES	NO	NO	YES
DYNAMIC ENVIRONMENT	NO	NO	NO	YES
FLEXIBILITY	NO	NO	NO	NO
KNOWLEDGE	NO	NO	NO	NO

5. Migration of RBAC to KC-RBAC

To protect patient information, RBAC models are being used currently. But there are some researches that suggest use of other technologies as well. Some technologies like Web Ontology language has also been used side by side to provide a patient with proper clinical diagnosis.
But points have been raised that even the knowledge about the medical domain should be taken into consideration. Knowledge and information can be taken from sources like ICD-10 and SNOMED CT which contain information about diseases, their relations and other various biomedical knowledge[10][13]. Therefore for the protection of patient privacy current models still need enhancement by integrating the knowledge of the medical domain in the present RBAC Model [10][13].
Since RBAC lets the user access data according to their rues there can be some discrepancy in it. For example, some authority working in the hospital system like management administration may also have access to patient data though they may have nothing to do with. Therefor it became necessary to include knowledge of the biomedical domain like clinical pathways etc. along with the RBAC model giving rise to KC-RBAC [10] [13].

6. Knowledge-Constrained Role Based Access Control Model and its Modules

KC-RBAC stands for Knowledge Constrained –Role Based Access Control Model. This combines the RBAC model but gives authority to roles according to their knowledge on the medical domain like clinical pathways etc.
The model consists of the following modules: General model, Knowledge model and the Purpose Tree [10][13]. The General Model consists the RBAC Model with an extension to the Knowledge Module. It maps the roles on the basis of the knowledge the user has in medical domain which it gets from the knowledge module and gives authority to user about it.
For example, a doctor needs to see the previous records of a patient for future use then he can see it. But similarly if a nurse has to view it she cannot as the nurse has nothing to obtain from previous records or give a diagnosis based on it since that is the doctor's job.



The knowledge module is the main machine that performs the reasoning of the system. It is the one that decides whether to give the user access or not on the basis of the information it derives from SNOMED CT along with ICD-10.
The Purpose Tree (PT) Module is another major component that elucidates the purpose as to why the user is visiting and asking for access of data based on the hierarchical tree structure[13].

7. Conclusion

As we have seen, the need of privacy for protection of patient details is a must in a Hospital Information System. One of the techniques involved in protection is Access Based Models. We have surveyed the various models that were adopted namely MAC, DAC and the most famous RBAC. But all had some shortcomings. To overcome these shortcomings many different extensions were performed as well on RBAC like the TRBAC, ABAC etc. But still the issue of privacy was not solved. Thus in recent studies a new implementation of RBAC was adopted which was called as the KC-RBAC. This took in detail the knowledge the user has related to the domain and only then it would provide the right to access. In comparison with the RBAC model and its different extensions, KC-RBAC can prove as an effective way of scrutinizing users and providing access due to its feature of the Knowledge Module. Due to the scrutinizing nature the patient privacy can be well preserved. Thus this model can have vast uses in other systems as well.

References

[1] Ebrahim Sahafizadeh, Saeed Parsa "Survey on Access Control Models"Volume 1 IEEE 2010
[2] Chen-Guang He , Cun-Zhang Cao and Shu-Di Bao "An Enhanced Role-Based Access Control Mechanism for Hospital Information Systems" IEEE Jan 2012
[3] Ruchika Asija and Rajarathnam Nallusamy "A survey on Security and Privacy of Healthcare Data" 2011.
[4] J. Li, "Ensuring privacy in a personal health record system," Computer, vol. 48, pp. 24-31, 2015.
[5] M. Fahim Ferdous Khan, Ken Sakamura "Towards a synergy among Discretionay, Role Based and Context Aware Access Control Model in Healthcare Information Technology" IEEE June 2012.
[6] Dipmala Salunke, Anilkumar Upadhyay, Amol Sarwade,Vaibhav Marde, Sachin Kandekar "A Survey Paper on Role Based Access Control" International Journal Of Advanced Research in Computer and Communication engineering Vol 2, Issue 3, March 2013.

[7] Min-A Jeong', Jung-Ja Kim', and Yonggwan Won"A Flexible Database Security System using Multiple Access Control Models" IEEE October 2003
[8] Lawrence Kerr, Jim Alves-Foss "Combining Mandatory and Attribute based Access Control" IEEE March 2016
[9] Deborah D. Downs, Jerzy R. Rub, Kenneth C. Kung, Carole S, Jordan "Issues In Discretionary Access Control" IEEE 2014
[10] R. Zhang, D. Chen, and X. Shang, "Privacy preserving for patients' information: a knowledge-constrained access control model for hospital information systems," In Proc. IEEE INDIN 2016, Poitiers, France, 2016, pp. 921-926.
[11] R. S. Sandhu, E. J. Coyne, H. L. Feinstein and C. E. Youman, "Rolebased access control models," IEEE Computer, vol. 29, pp. 38-47, 1996.
[12] Barsha Mitra , Shamik Sural, Jaideep Vaidya , Vijayalakshmi Atluri "Migrating from RBAC to Temporal RBAC" IEEE Aug 2017
[13] Runtong Zhang, Senior Member, IEEE, Donghua Chen, Xiaopu Shang, Member, IEEE, Xiaomin Zhu, and Kecheng Liu "A Knowledge-Constrained Access Control Model for Protecting Patient Privacy in Hospital Information Systems" IEEE 2017.
[14] Lindi A. Slevin, Alex Macfie "ROLE BASED ACCESS CONTROL FOR A MEDICAL DATABASE" ACM Digital Library 2007
[15] Bokefode Jayant, Ubale Swapnaja, Modani Dattatray, Apte Sulabha S. "Analysis of DAC MAC RBAC Access Control based Models for Security" International Journal of Computer Applications (0975 – 8887) Volume 104 – No.5, October 2014
[16] T. Padmapriya, V.Saminadan, "Performance Improvement in long term Evolution-advanced network using multiple imput multiple output technique", Journal of Advanced Research in Dynamical and Control Systems, Vol. 9, Sp-6, pp: 990-1010, 2017.
[17] S.V.Manikanthan and K.Baskaran "Low Cost VLSI Design Implementation of Sorting Network for ACSFD in Wireless Sensor Network", CiiT International Journal of Programmable Device Circuits and Systems,Print: ISSN 0974 – 973X & Online: ISSN 0974 – 9624, Issue : November 2011, PDCS112011008.