Role-Based Access Control Requirements Model with Purpose Extension

Faranak Farzad[1], Eric Yu
Faculty of Information Studies
University of Toronto, Canada
Patrick C. K. Hung
Faculty of Business and Information Technology
University of Ontario Institute of Technology, Canada
[1]*farzad@fis.utoronto.ca*

Abstract

Role-Based Access Control (RBAC) is increasingly used for ensuring security and privacy in complex organizations such as healthcare institutions. In RBAC, access permissions are granted to an individual based on her defined roles. Much work has been done on the specification of RBAC models for enforcing access control; however, in order to arrive at appropriate choices of access control for particular roles and individuals in an organization, we need models at the requirements level to support elicitation and analysis.

Crook et al. [3] have provided a requirements level model for RBAC, defining access to an information asset based on role, responsibility, operation, and context. We extend the Crook model to include a purpose hierarchy in order to meet the needs of privacy requirements. Access to health records is used as the example domain.

1. Introduction

Access to information could be abused in organizations that keep important information. Therefore, it is necessary to ensure that the behavior of the users does not compromise security goals in any system [3]. System designers usually start thinking about access control policy during the last phases of system development, despite its importance [3]. Particularly, this occurs in the healthcare system where security of patients' data is one of the most important concerns of both the patients and the healthcare providers. It is important to address access control policy early on in the development of any healthcare system [3]. In Canada, based on the Personal Health Information Protection Act (PHIPA) [13], patients have the right to know who can read their information and who can make changes to it. Moreover, patients are able to further restrict access to their profile by asking the healthcare system to block specific people.

In some systems, it is possible to break down activities to smaller tasks, which can then be assigned separately to individuals. This technique prevents individuals from defrauding the system [10]. However, in some systems such as in healthcare, it is not possible to divide responsibilities and assign to separate individuals. In order to provide the best treatments to the patients, medical practitioners need to be aware of the patient's status during all phases of the treatment and have access to his/her complete information.

Role-Based Access Control (RBAC) provides a finer-grain specification of access control based on the roles that are taken on by individuals [8, 9]. Much work on RBAC models have focused on the specification of models for enforcement. However, in order to determine the correct choices of access control for particular roles in an organization, we need models at the requirements level to allow analysis. For example, Crook *et al.* [3] have provided RBAC models at the requirements level.

RBAC models were originally created with security in mind. Recent privacy legislations introduce new requirements that are not covered in RBAC, such as the explicit treatment of purpose. Cheng and Hung [1] have proposed an extended RBAC model to specify policies with purpose. In this paper, we propose RBAC requirements models to include purpose by extending Crook's work.

The paper is organized as follows. Section 2 explains RBAC and its limitations using examples from healthcare systems. Section 3 discusses RBAC with privacy extension and how it overcomes some of the problems associated with RBAC [1]. Some of the drawbacks of RBAC with privacy extension in the requirement level are also described. In section 4, we introduce a revised version of RBAC that addresses some of the problems of the two previous techniques. Section 5 concludes the paper with a short summary and discussion of possible future work.

2. Role-Based Access Control

There are different types of access control such as user-based, task-based, team-based, or role-based access control [5, 10, 11]. Each of these techniques is suitable for a specific type of system. Some are used for simple organizations, whereas others are used for more complex ones. Role-based access control models provide the fine-grained control needed in complex organizations such as healthcare systems [13].

Since 1996, research on access control policy has been focused more on RBAC [8]. In RBAC, permission is given to the roles rather than the users. Roles need to be defined to be mutually exclusive in order to maximize security of the system. There are different types of RBAC techniques [3, 6, 7, 9]. Below, we explain some of these techniques and highlight their pros and cons.

In 2000, Sandhu *et al.* introduced NIST (National Institute of Standards and Technology) RBAC models [9]. Similar to the other RBAC models, permissions are given to the roles rather than the users, where roles are defined to be mutually exclusive. The authors introduced two types of hierarchies – a role hierarchy and an activity hierarchy. In the role hierarchy, senior roles inherit all permissions of junior roles, whereas in the activity hierarchy senior roles inherit only partial permissions of junior roles.

Moffett [6, 7] extended the NIST RBAC model to make it more suitable for complex organizations. He introduced an RBAC model, with three types of hierarchies; *is-a*, *activity*, and *supervision*. For instance, in the healthcare system, one can create a role called healthcare provider who has all the responsibilities common among nurses, physicians, and lab technicians (See Fig. 1). By giving a set of permissions to healthcare providers, the nurses, physicians, and lab technicians also inherit the same set of permissions. Moffett called this type of hierarchy *is-a* and the relationship can be read as: a physician/nurse/lab technician *is-a* healthcare provider.

Activity hierarchy connects the roles that are needed to perform a task. For example, only a physician who is responsible for a patient can give prescription to him/her. Supervision hierarchy connects senior roles to junior ones. For instance, nurse to a head nurse.

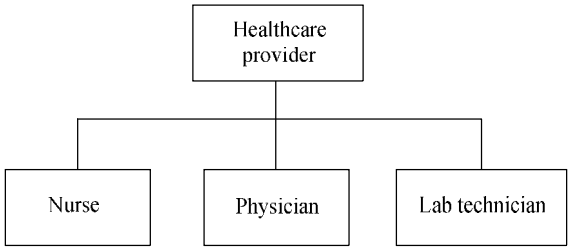

Fig. 1: Is-a hierarchy connects the healthcare providers to nurses, physicians, and lab technicians.

Covington *et al.* [2] added another type of permission to the RBAC that is based on the environment. This type of permission is not required in systems such as healthcare where the healthcare providers have access to patients' medical information anywhere and anytime there is a need to.

Crook [3] defined roles and categorized them as follows: functional role, seniority role, and contextual role (See Fig. 2). Access is defined as a relation among users, roles, operations, and assets. In other words, if a user has certain role(s), he/she can do specific operations on one or more assets. A contextual role is connected to a context type where it is connected to an asset [3]. Fig. 3 shows an example where a doctor (role) has a read and write (operation) access to a patient's medical record (asset), provided that the doctor is responsible (role) for that patient (context).

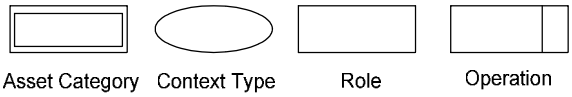

Fig. 2: Policy Definition [3]

Crook identifies three types of hierarchies where the ones between functional roles or asset categories represent inheritance (See Figs. 4 and 5) [3, 13]. The more general roles/assets are at the top while the more specific ones are at the bottom of the model.

For seniority roles, hierarchy shows line of authority [3].

Hierarchies enable policies to be defined at any necessary detail. General policies can be defined using the assets and roles in the top levels of the hierarchy, whereas more specific policies can be defined by the assets and roles in the lower levels. For instance, in healthcare systems, physicians, nurses, and lab technicians inherit permissions of the healthcare provider [13]. Moreover, patients' progress reports, lab results, and general information inherit permissions from patients' information [13]. Hence, a policy that is related to the patients' information and the healthcare providers, also applies to nurses/physicians/lab technicians and patients' progress report/ lab result/ patients' general information.

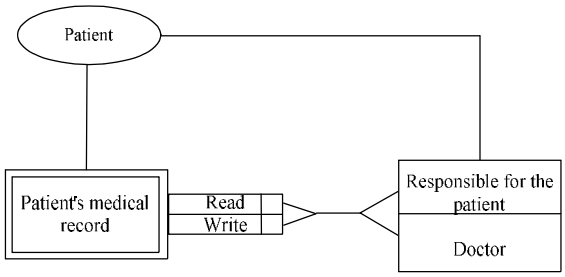

Fig. 3: The doctor who is responsible for the patient has read and write access to a patient's medical record [3].

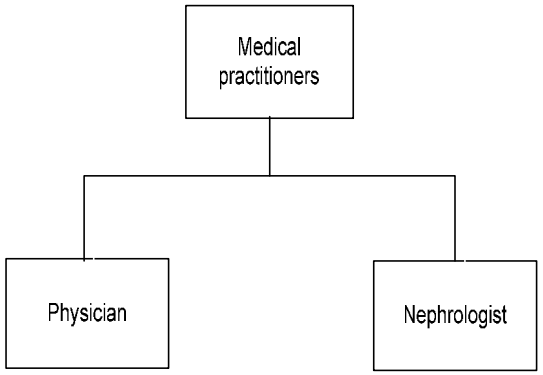

Fig. 4: Functional role hierarchy: a physician or a nephrologist inherits permissions of the medical practitioner role.

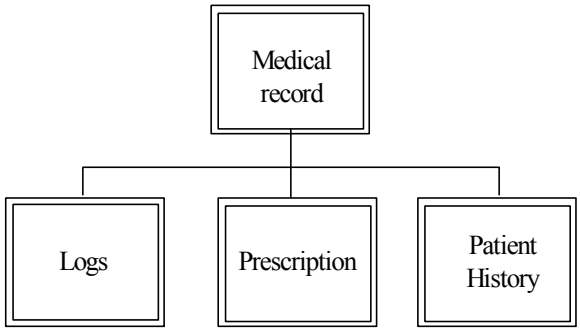

Fig. 5: Asset hierarchy, Patients' medical record can be logs, prescription, or patient history. The policies that are applied to the medical records are also applied to log prescription and patients' history.

In order to use Crook's RBAC technique, one has to consider that the purpose of an individual in requesting access is not included in Crook's role-based access control. Individuals may want to have access to different information for different purposes. Therefore, the type of access they get should change depending on their purpose. For instance, a physician may require access to a patient's information. His/her purpose can be to give a prescription to the patient or to complete the patient's profile. In the first case, the system can give read access to the physician. However, in the second case, the physician should also be able to add or change the patient's profile as well. Therefore, access control should be able to give different types of accesses in the two cases. Crook's models are not able to put purpose into considerations.

3. RBAC with privacy extension

Cheng and Hung introduced RBAC with privacy-based extension [1] that provides the specification for enforcement. In their formulation, a request for permission includes subject, object, operation, purpose, and recipient while a response includes the given permission, set of obligation, and retention [1].

Access is defined as follows: Suppose there is a set of objects O: $\{o_1, o_2, \ldots, o_i\}$, purposes PP: $\{pp_1, pp_2, \ldots, pp_j\}$, recipients RP: $\{rp_1, rp_2, \ldots, rp_k\}$, obligation OB: $\{obl_1, obl_2, \ldots, obl_m\}$, and retention RT: $\{rt_1, rt_2, \ldots, rt_i\}$. If subject s can do operation ops on a set of objects for any purpose pp_k $\{pp_k \mid 0<k<j+1\}$ and any recipient in RP, then a set of obligation, OB and a set of retention RT are returned to s. If subject s is not authorized then the result

{Deny, {}, {}} is returned to s. Note that when access is denied, the two sets of retention and obligation are empty.

Below, we demonstrate how to apply the RBAC model with privacy extension developed by Cheng and Hung [1] to the healthcare system. In the next section, we will use similar examples for illustrating a requirements level of RBAC model with purpose extension.

3.1. Example: right to review and change

The right to review and make changes to patient's file can be described as follows [12, 13]:

A physician responsible for a patient has the permission to review and change the patient's General Information, Medical practitioners' Orders, Patients' History, Progress Report, and Lab Result. This is, provided that the purpose of reviewing or changing the above information falls in one of these categories: Correction of inaccurate information, Adding information, Review patients' History before giving treatment, or Contact patients' families.

After getting the permission, the physician will gain some responsibilities as follow: He/she is not allowed to discuss the patient's health information with him/her if the information in question is subject to legal privilege, if its disclosure could reasonably be expected to result in a risk of serious bodily harm to a patient, or if the information is collected as part of the investigation. Moreover, the physician can only review and change the information while he/she is responsible for the patient. The physician must also refer the patient to the specialist and order lab tests if necessary.

In the following, we describe how one can demonstrate the above scenario using Cheng and Hung's RBAC with privacy extension technique [1].

$\forall s_j \in$ SUBJECTS, subject_users$(s_j) \not\subset \varnothing$
r = "Patient" $\in$ subject_role $(s_j) \subseteq$ ROLES
$\forall s_i \in$ SUBJECTS, subject_users$(s_i) \not\subset \varnothing$
r = "Physician" $\in$ subject_role $(s_i) \subseteq$ ROLES
subject_users $(s_i) \in$ assigned_user(r)

op_1 = review, op_2 = write, $\{op_1, op_2\} \subseteq$ OPS

o_1 = Patient's General Information
o_2 = Medical practitioners' Orders
o_3 = Patients' History and Progress Report
o_4 = Lab Result

$\{o_1, o_2, o_3, o_4\} \subseteq$ owner_object (s_i)
pp_1 = Correction of inaccurate information
pp_2 = Adding information
pp_3 = Review patients' History before giving treatment
pp_4 = Contact patients' families (when Personal Health Information Protection Act allows)

$\{pp_1, pp_2, pp_3, pp_4\} \subseteq$ PURPOSES

obl_1= Do not discuss a patient's health information with her/him if the information in question is subject to legal privilege
obl_2 = Do not discuss a patient's health information with her/him if its disclosure could reasonably be expected to result in a risk of serious bodily harm to a patient
obl_3 = Do not discuss a patient's health information with her/him if the information is collected as part of the investigation

$\{obl_1, obl_2, obl_3\} \subseteq$ OBLIGATION

rt_1= Physician can review and change information as long as he/she is responsible for the patient.
rt_2= While responsible for the patient the physician should refer the patient to the specialist if needed.
rt_3= While responsible for the patient the physician should order lab tests that he/she needs to know in order to make decision.

$\{rt_1, rt_2, rt_3\} \subseteq$ RETENTIONS

$s_i \in$ RECIPIENTS i.e. RECIPIENTS={Physician, Patient}
$\Rightarrow$

Access $(s_j$, OPS, $\{o_1, o_2, o_3, o_4\}$, PURPOSES, $s_i)$ = (ALLOW, OBLIGATIONS, RETENTIONS)

3.2. Example: right to review

The right to review patient's file [12, 13]:

A medical practitioner who is responsible for a patient has the permission to review medical practitioners' orders, the patient's history, and progress report if his/her purpose of reviewing the above information is: correction of inaccurate information, adding information, or carrying out Physicians' orders.

After getting the permission, the physician gains the following responsibilities: Medical practitioner

cannot discuss patients' health information with her/him if the information in question is subject to legal privilege, if its disclosure could reasonably be expected to result in a risk of serious bodily harm to a patient, or if the information is collected as part of the investigation. Moreover, the medical practitioner has to carry out the orders written by physicians and make corrections if anything is inaccurate or missing, and update patient's medical record based on his/her observation.

In the following we describe how one can demonstrate the above scenario using Cheng and Hung's RBAC with privacy extension technique [1].

$s_j \in$ SUBJECTS, subject_users$(s_j) \not\subset \varnothing$
r = Patient $\in$ subject_role $(s_j) \subseteq$ ROLES

$s_i \in$ SUBJECTS, subject_users$(s_i) \not\subset \varnothing$
r = Medical Practitioner $\in$ subject_role $(s_i) \subseteq$ ROLES

subject_users $(s_i) \in$ assigned_user(r)

op_1 = review $\{op_1\} \subseteq$ OPS

o_1= Medical practitioners' Orders
o_2= Patients' History and Progress Report
$\{o_1, o_2\} \subseteq$ owner_object (s_i)

pp_1 = Correction of inaccurate information
pp_2 = Adding information
pp_3 = Doing Physicians' orders

$\{pp_1, pp_2, pp_3\} \subseteq$ PURPOSES

obl_1 = Do not discuss the patient's health information with him/her if the information in question is subject to legal privilege
obl_2 = Do not discuss the patient's health information with him/her if its disclosure could reasonably be expected to result in a risk of serious bodily harm to a patient
obl_3 = Do not discuss the patient's health information with him/her if the information is collected as part of the investigation

$\{obl_1, obl_2, obl_3\} \subseteq$ OBLIGATION

rt_1 = While responsible for the patient, conduct the orders written by physicians.
rt_2 = While responsible for the patient, make corrections if anything is inaccurate or missing, and update patient's medical record based on your observation
$\{rt_1, rt_2\} \subseteq$ RETENTIONS

$s_i \in$ RECIPIENTS i.e. RECIPIENTS={Medical practitioner, Patient}
$\Rightarrow$
Access $(s_j$, OPS, $\{o_1, o_2\}$, PURPOSES, $s_i)$ =
(ALLOW, OBLIGATIONS, RETENTIONS)

The Cheng & Hung [1] privacy extension to RBAC provides a mathematical specification for enforcement. In the next section, we include purpose into RBAC from a requirements engineering viewpoint, by extending the Crook notation.

4. RBAC with purpose extension

The key components of RBAC with purpose extension framework are the same as Crook's RBAC framework but it also includes purpose entity (See Fig. 6). In Fig. 7, the area that is bounded by the dashed circle contains the new entities.

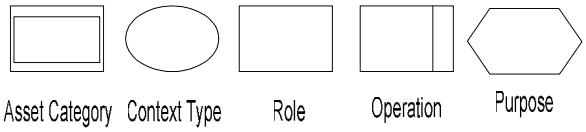

Fig. 6: Policy definition

4.1. Adding purpose to RBAC models

Similar to other RBAC models, permissions are given to the roles where the roles are defined to be mutually exclusive. There are still functional roles, seniority roles, and asset hierarchies. In addition, purpose hierarchy is added to the models where purposes are defined to be mutually exclusive. Purpose hierarchies are similar to asset hierarchies, where the upper levels include general purposes and the lower levels include more specific ones. Therefore, in Fig. 8 any policy that applies to the purpose, *give treatment*, the same set of policies would apply to both *refer patient to specialist* and *write prescription*. In Fig. 10 any policy that applies to the purpose, *complete patient profile,* the same set of policies would apply to *complete patient history*, *add order*, and *request a test*. In Fig. 12 any policy that applies to the purpose, *discuss with others,* the same set of policies would apply to *discuss with a colleague*, *discuss with patient's family*, and *discuss with patient him/herself*.

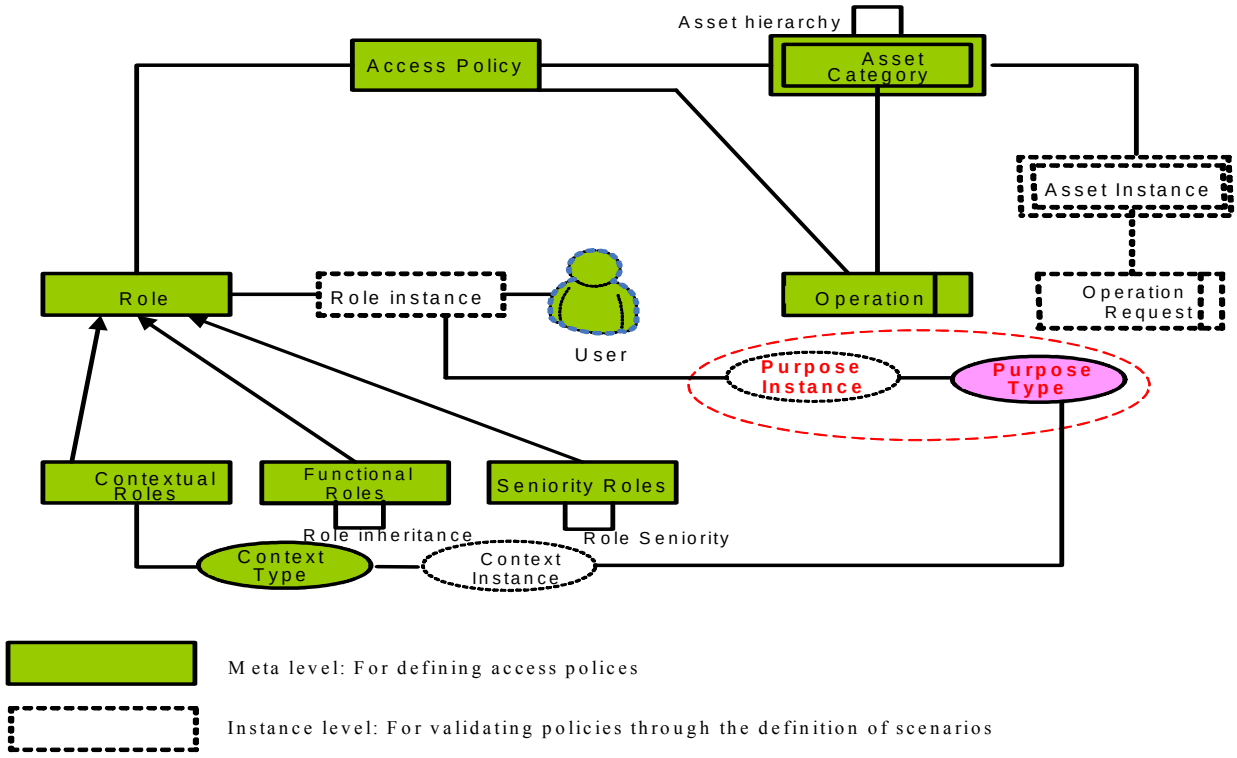

Fig. 7: The Key component of the framework

4.2. Some examples from healthcare

In this section, we demonstrate how to apply RBAC with privacy extension to the healthcare system using similar examples as those in section 3. Suppose that the roles and assets hierarchies are defined the same as Figs. 4 and 5 where a medical practitioner, responsible for the patient, can only review the patient's medical record if the medical practitioner wants to give treatment to the patient (see Fig. 9). However if the medical practitioner wants to complete the patient's profile, she/he is also able to review and make changes to the patient's medical record (see Fig. 11). If a medical practitioner who is responsible for the patient wants to discuss the patient's case with others, she/he can review patient's profile, but cannot make any changes to it (see Fig. 13). In this example, one can see that it is not possible to define access control without including an entity for purpose.

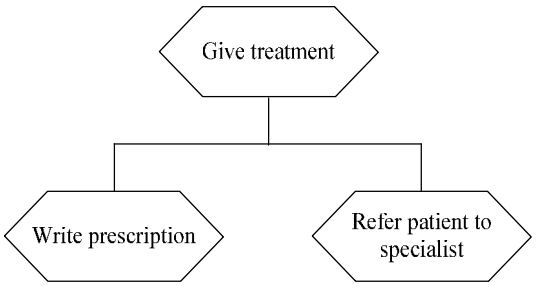

Fig. 8: Purpose hierarchy: Any policy that applies to the purpose, *give treatment*, the same set of policy would apply to both *refer patient to specialist* and *write prescription*.

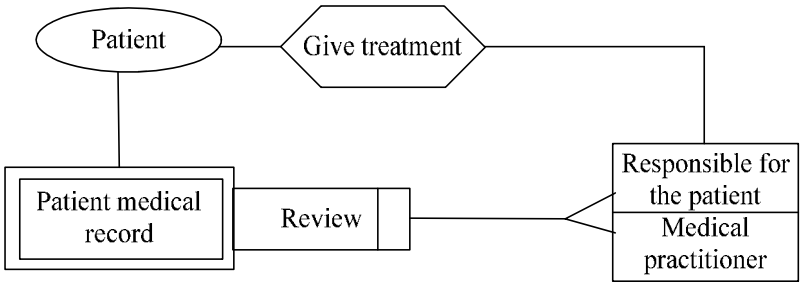

Fig. 9: A medical practitioner who is responsible for the patient can only review the patient's profile if she/he wants to give treatment to the patient.

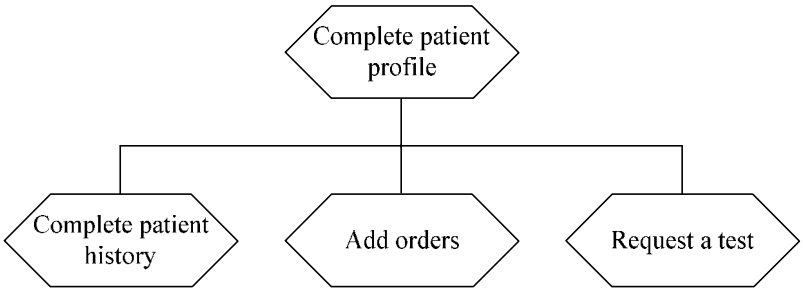

Fig. 10: Purpose hierarchy: Any policy that applies to the purpose, *complete patient profile*, would apply to *complete patient history, add order,* and *request a test*

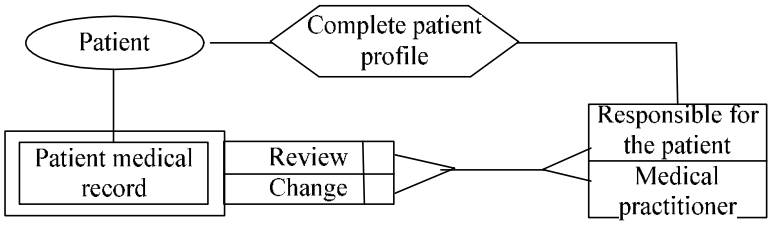

Fig. 11: If the medical practitioner wants to complete patient's profile, she/he has the permission to review and make changes to patient's medical record

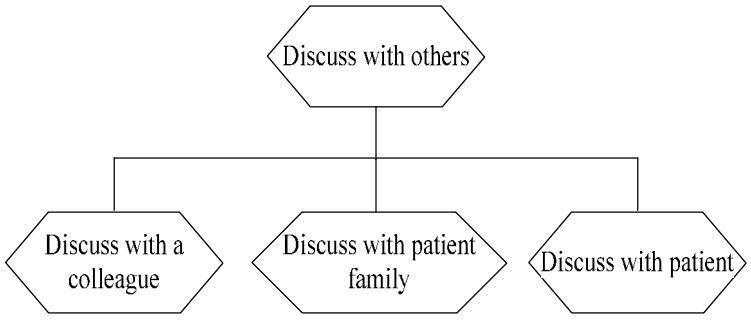

Fig. 12: Purpose hierarchy: Any policy that applies to the purpose, *discuss with others,* the same set of policies would apply to *discuss with a colleague*, *discuss with patient's family*, and *discuss with patient him/herself*.

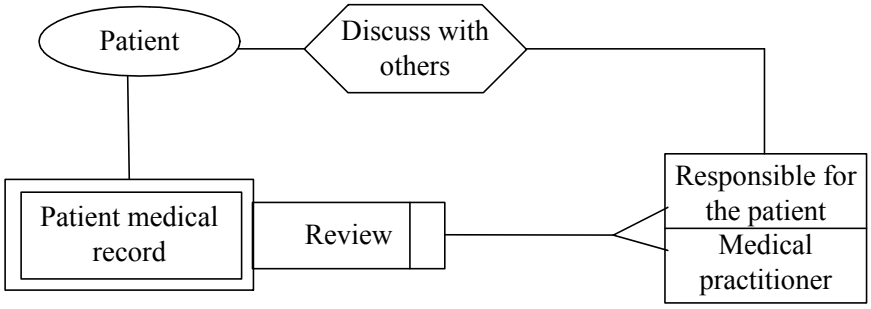

Fig. 13: If a medical practitioner wants to discuss the patient's profile with others, she/he has the permission to review the patient's medial record.

Below, three different scenarios are explained regarding access control in healthcare systems. In the first scenario, the healthcare access policy is investigated in the high level. In the second and third ones, the models explore access policy for more specific cases.

Case 1: Rose Biel who is a medical practitioner and is responsible for the patient, Michelle Smith, wants to complete Michelle's profile so, Rose would get the permission to review and change Michelle Smith's medical record (see Fig. 14).

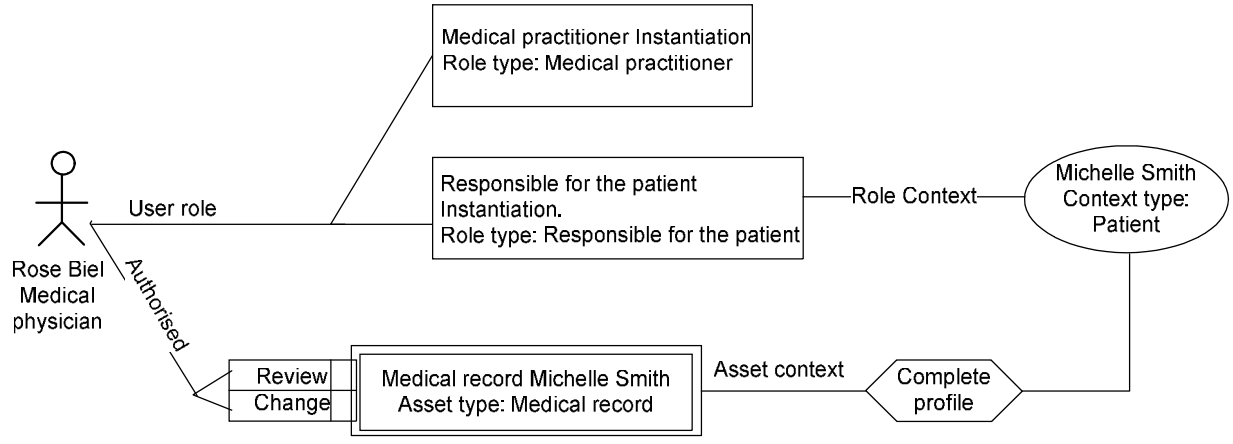

Fig. 14: Biel wants to complete Michelle's profile (an instantiation of Fig. 12)

Case 2: Rose Biel who is a nephrologist, responsible for the patient Michelle Smith, wants to refer Michelle to a specialist. Therefore Rose would have the permission to change (add to) Michelle Smith's medical history but she is not allowed to read her profile (see Fig. 15)

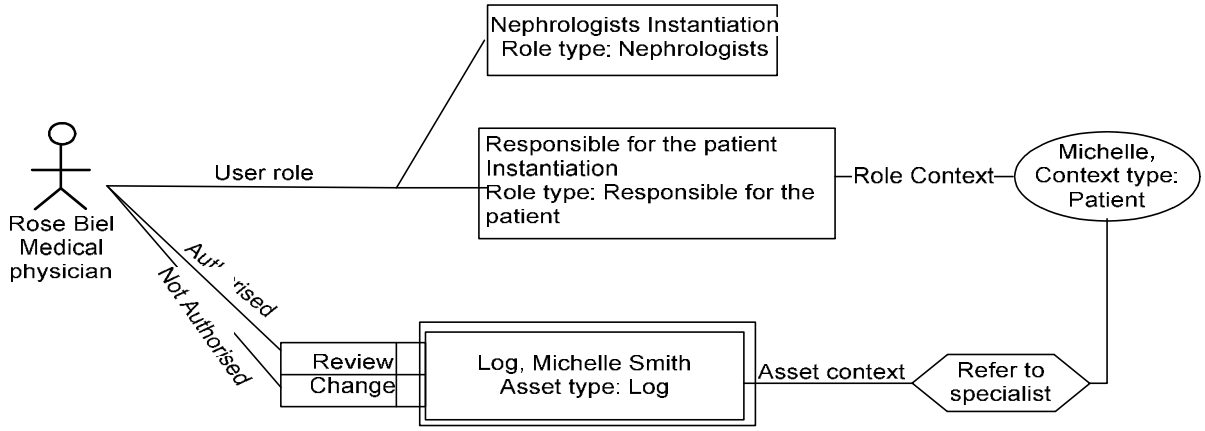

Fig. 15: Rose Biel wants to refer Michelle to a specialist

Case 3: Rose Biel who is a nephrologist and is responsible for the patient, Michelle Smith, wants to add order to Michelle's medical history. Therefore, Rose would get the permission to both change and review Michelle Smith's medical history (see Fig. 16).

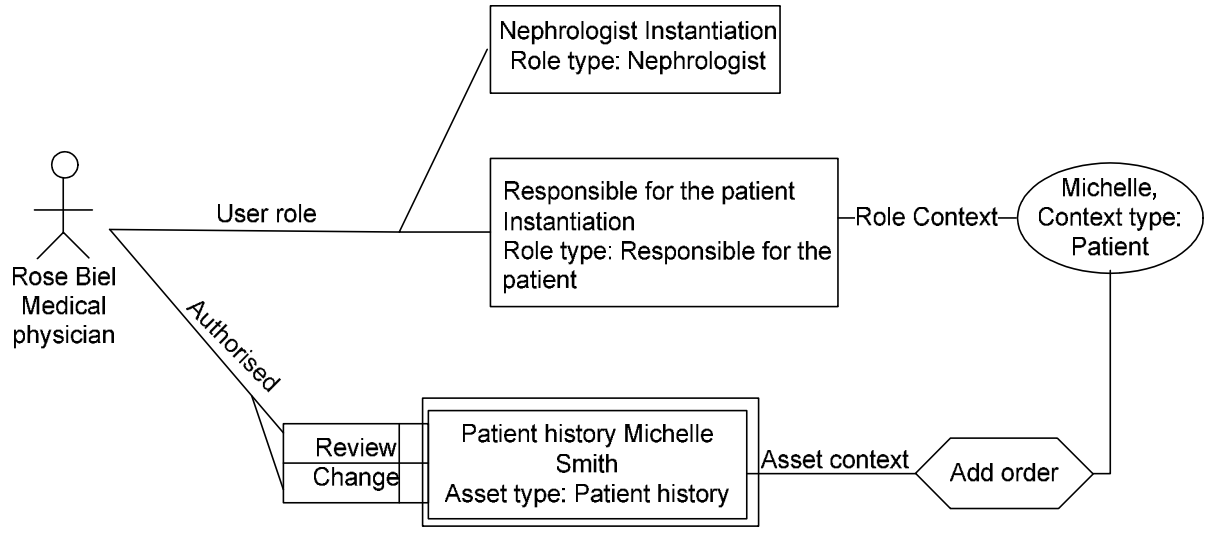

Fig. 16: Rose Biel wants to add order to Michelle's medical record.

5. Conclusion:

Earlier RBAC models have some limitations; for example, it does not include purpose and therefore, cannot distinguish between scenarios where the healthcare providers need information for different purposes. This problem has been addressed in RBAC models with privacy extension. In this paper, we introduced requirements level RBAC models with a purpose hierarchy. In future work, obligation and retention hierarchies can be added. Obligation and retention specify the responsibility of the information user after giving access to them. In this paper, we have not included obligation and retention as they do not have any effect on the type of access the individual will get. For a more complete privacy requirements model, obligation and retention can be added, following Chen and Hung's RBAC with privacy extension.

6. Acknowledgements

Financial support from the Bell University Laboratories is gratefully acknowledged. Thanks also go to Michelle Watson for improving the presentation of the paper.

References

[1] V. S. Y. Cheng, P. C. K. Hung, , Health Insurance Portability and Accountability Act (HIPAA) Compliant Access Control Model for Web Services, *International Journal of Healthcare Information Systems and Informatics*, Vol 1, Issue 1,2005, pp. 22 - 39

[2] M.J. Covington, W. Long, S. Srinivasan, A.K. Dev, M. Ahamad, G.D. Abowd, Securing context-aware applications using environment roles, *Proceedings of the 6th ACM Symposium on Access Control Models and Technologies*, May 2001, pp. 10–20

[3] R. Crook, D. Ince, B. Nuseibeh, Modeling access policies using roles in requirements engineering, *Information and Software Technology (Elsevier)* 45(14), November, 2003, pp. 979-991.

[4] A. Finkelstein, J. Dowell, "A comedy of Errors: The London Ambulance Service Case Study" *Proceedings of the Eighth International Workshop on Software Specification and Design,* IEEE Computer Society Press pp 2-5 1996

[5] C.K. Georgiadis, I. Mavridis, G. Pangalos, R.K. Thomas, Flexible team-based access control using contexts, *Proceedings of the 6th ACM Symposium on Access Control Models and Technologies*, May 2001, pp. 21–27.

[6] D. Moffett, Control principles and role hierarchies, *Proceedings of the 3rd ACM Symposium on Access Control Models and Technologies*, October 1998, pp. 63–69.

[7] J.D. Moffett, Control principles and role hierarchies, *Proceedings of the 3rd ACM Symposium on Access Control Models and Technologies*, October 1998, pp. 63–69.

[8] R. Sandhu, E. Coyne, H. Feinstaein, C. Youmann, Role-based access control models, IEEE Computer 29 (2) (1996) 38–47.

[9] R. Sandhu, D. Ferraiolo, R. Kuhn, The NIST model for role-based access control: towards a unified standard, Proceedings of the 5th ACN Workshop on Role-Based Access Control (RBAC-00), Berlin Germany, July 26–27 (2000) 47–64.

[10] R. Thomas, R. S. Sandhu, Conceptual foundations for a model of task-based authorizations. In *Proceedings of 7th IEEE Computer Security Foundations Workshop*, Franconia, NH. 1994. pp. 66–79.

[11] W. Tolone , G. J. Ahn , T. Pai , S. P. Hong, Access control in collaborative systems, *ACM Computing Surveys (CSUR)*, v.37 n.1, p.29-41, March 2005

[12] M. Watson, Mobile Healthcare Applications: A Study of Access Control, *Proceedings of the Fourth Annual Conference on Privacy, Security and Trust (PST'2006),* 2006, pp. 525-528.

[13] Information and privacy commissioner (Ontario) Retrieved Aug. 10, 2006, from http://www.ipc.on.ca/