Towards an Access Control Model for Collaborative Healthcare Systems

Mohamed Abomhara and Geir M. Køien
Department of Information and Communication Technology, University of Agder, Grimstad, Norway

Keywords: Access Control, Authorization, Electronic Health Records, Security, Privacy, Collaborative Healthcare Systems.

Abstract: In this study, an access control model for collaborative healthcare systems is proposed. Collaboration requirements, patient data confidentiality and the need for flexible access for healthcare providers through the actual work they must fulfill as part of their duties are carefully addressed. The main goal is to provide an access control model that strikes a balance between collaboration and safeguarding sensitive patient information.

1 INTRODUCTION

Healthcare services necessitate collaborative support from multiple parties to fulfill the information requirements of daily clinical care and provide rapid patient care (Moonian et al., 2008). Collaborative support is required within healthcare organizations such as hospitals, where patient records must be moved among healthcare professionals, laboratories and wards, to name a few. Collaboration among healthcare organizations is also essential for patients being transferred from one healthcare provider to another for specialized treatment. Such collaboration within or among healthcare organizations has been shown to provide cost-effective healthcare services (Alshehri and Raj, 2013). However, collaboration and information sharing raise security and privacy concerns (Gajanayake et al., 2014). Patient records contain sensitive information that calls for appropriate access control mechanisms to ensure confidentiality and protect integrity of data as well as filter out irrelevant information to reduce information overload (Alhaqbani and Fidge, 2008).

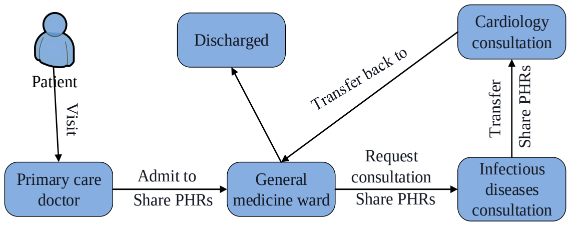
Access control is defined as a mechanism through which users are permitted access to resources according to their identities (authentication) and associated privileges (authorization) (Hu et al., 2006). Access control mechanisms have undergone many developments in both academia and industries in order to meet healthcare domain needs. However, progress to date has not been sufficient to fulfill the security requirements of a collaborative healthcare environment (Alhaqbani and Fidge, 2008). The majority of models, such as Role-Based Access Control (RBAC) (Ferraiolo et al., 2001) and Attribute-Based Access Control (ABAC) (Hu et al., 2014) for instance, help restrict medical records to users based on certain roles and attributes, but sensitive information can still be compromised by authorized insiders (Alshehri et al., 2013; Alshehri and Raj, 2013; Ferreira et al., 2007). Such models and extensions have been employed in specific applications to manage information access in a controlled environment. Nevertheless, few studies have addressed the issue of managing information access within the context of team collaboration (Thomas, 1997; Georgiadis et al., 2001; Alotaiby and Chen, 2004) and workflow (Le et al., 2012; Russello et al., 2008). This study, proposes an access control model that is secure, flexible, easy to manage, and supports cooperative engagements. Our focus is mainly on collaborative activities that are best accomplished through organized groups of healthcare practitioners within or among healthcare organizations with the objective of accomplishing a specific work (treatment of patient's case).

1.1 Collaboration and Secure Sharing of Healthcare Data

Healthcare providers deal with large amounts of sensitive healthcare records which are shared and collaboratively used among different healthcare practitioners (Fabian et al., 2015). Collaboration occurs when a healthcare provider such as primary care doctor requests help from another healthcare provider to treat a case. Figure 1 provides an example scenario of collaboration and sharing of healthcare data.

In this scenario, a 7-year old patient visited his primary care doctor with high body temperatures. The

Abomhara, M. and Køien, G.
Towards an Access Control Model for Collaborative Healthcare Systems.
DOI: 10.5220/0005659102130222
In *Proceedings of the 9th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2016) - Volume 5: HEALTHINF*, pages 213-222
ISBN: 978-989-758-170-0



PHRs : Patient Healthcare Records

Figure 1: An example scenario of collaboration and sharing of healthcare data.

patient was quickly examined by the primary care doctor and the cause of fever could not be found. The patient was admitted to the general medicine ward, where he was reassessed by the attending physician who requested some routine blood tests. Upon admission, the attending physician subsequently requested an infectious diseases consultation because the patient begun to develop a skin rash. The infectious diseases team investigated further and decided to consult the cardiology team as they were concerned about Kawasaki disease. The patient was immediately transferred to the cardiology ward. Eventually, the patient made a substantial recovery and was transferred back to general medicine ward. After spending a few more days in the hospital, the patient has recovered, then he was discharged, and advised to see his primary care doctor for follow-up.

In such group consultation, it is noticed that, several healthcare professionals are involved in various roles to provide patient care. That includes primary care doctors, general physicians and specialists such as the infectious diseases team and cardiologists. Every participant needs to obtain the medical records they request based on the health insurance portability and accountability act (HIPAA) minimal disclosure principle (Zhang and Liu, 2010; Fabian et al., 2015). Therefore, sharing and accessing healthcare records with efficient coordination between healthcare practitioners to perform collaborative work is a critical function in access control models (Alotaiby and Chen, 2004). The main concern is about losing control over the sensitive healthcare records while sharing them with multiple parties. Many researches (Shen and Dewan, 1992; Thomas, 1997; Rubio-Medrano et al., 2013) have developed access control models to support collaborative requirements by defining a set of rules in the subject, objects and access rights dimensions. However, these models are general and quit complex. Additionally, they do not present an applicable solution for collaborative healthcare system.

The remaining parts of this study is structured as follows: section 2 discusses the insider threat problem in the health domain and presents an overview of the existing access control models. In section 3, the proposed access control model is introduced. Conclusions and future works are suggested in section 4.

2 BACKGROUND

In this section, a brief overview of the insider threat problem in the healthcare domain is presented along with existing access control models and their pros and cons with respect to health systems.

2.1 Insider Threat

As shown in our scenrio (Fig.1), healthcare services need the collaborative support of multiple healthcare professionals and administrators in order to deliver rapid patient care. Therefore, multiple users (e.g. doctors and nurses) may require access to patient information to perform tasks. For this reason, insider abuse or misuse of privileges (Probst et al., 2010) can be a threat to patient information and a liability for health care providers. One of the main causes of insider threats in collaborative healthcare is information leakage, which emerges when a supporting party is granted access beyond what is actually required (Figure 2 (a)). For instance, in treating a patient case, the main practitioner consults a specialist from another department. In doing so, improper information access might occur if the specialist (e.g. cardiologist) obtains more permission than required. The key to solving this issue is to minimize the discrepancy (Figure 2 (b)) between the granted access and the required access based on what is really needed.

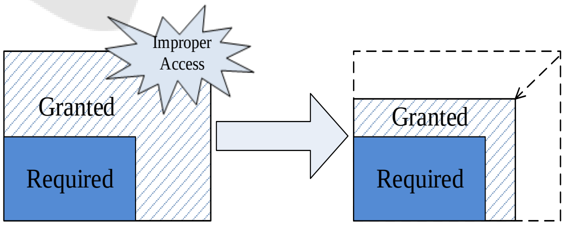


Figure 2: (a) Granted vs required information access and (b) Minimization of access discrepancy.

2.2 Access Control Models

Research in security area has made every possible effort to address security challenges related to authorization and access control. In this section, existing access control models are discussed, and their strengths and weaknesses are identified with respect to healthcare systems.

2.2.1 Discretionary Access Control (DAC)

DAC (Hu et al., 2006; Kayem et al., 2010; Samarati and Di Vimercati, 2001) defines access control privileges based on the subject's identity and the access rules in place. It determines whether the subject can or cannot execute particular actions on specific resources (objects or files). DAC allows the subject to own resources and for ownership to be transferred to another subject (Majumder et al., 2014). Although DAC policies tend to be flexible and are widely deployed, DAC has several drawbacks when utilized in healthcare systems (Alhaqbani and Fidge, 2008; Gajanayake et al., 2014). First, ownership and permission updating is not scalable, as the number of users and medical records are continuously growing. Second, DAC policies do not provide high security assurance, because granting read access is transitive and, DAC allows data to be copied from one resource to another, which can result in unintentional information flow in a system (Hu et al., 2006).

2.2.2 Mandatory Access Control (MAC)

In MAC (Samarati and Di Vimercati, 2001; Hu et al., 2006; Majumder et al., 2014), a subject cannot change the access rights to objects because access control policy decisions are made by a central authority. Unlike DAC, MAC controls information flow to ensure information confidentiality and integrity (Kayem et al., 2010). However, enforcing MAC policies in healthcare systems is often very difficult due to the vast numbers of users, the wide range of data types, and the requirements to give patients control ownership of their own medical records.

2.2.3 Role-based Access Control (RBAC)

RBAC (Ferraiolo et al., 2001) allows organizations to enforce access policies based on subjects' roles (job functions) rather than users or groups, as shown in Figure 3.

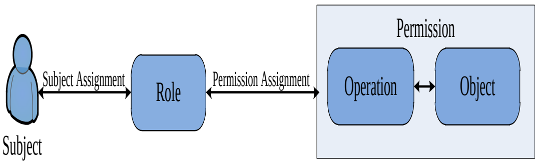


Figure 3: Overview of the RBAC model.

Subjects (users) are assigned roles (e.g. patient, doctor, or nurse), permissions (or access rights) are then grouped based on the roles. Access to resources (medical records in this case) is restricted to authorized individuals according to the assigned roles. RBAC has a number of advantages, including flexibility in terms of permission administration management, since roles can be updated without updating permissions for every user. Moreover, the use of role hierarchies provides additional advantages, as one role may implicitly include operations associated with another role. Also, the separation of duties (SoD) principle ensures that no user is allowed to execute two roles simultaneously. Although the RBAC model has several advantages, it also has disadvantages. That is why it is not efficiently implemented in healthcare environments. Insider threats are a common problem faced by healthcare systems due to RBAC's lack of granularity (Alshehri and Raj, 2013). Roles are not sufficiently granular to restrict data access to only the right (authorized) subjects. For example, consider a role that is associated with a set of permissions. Any subject in this role would be allowed the permissions associated with this role (Alshehri et al., 2013). Furthermore, RBAC does not consider healthcare provider workflow (Russello et al., 2008) nor separate task from role. Various types of tasks with different access control characteristics are dealt with in the same manner (Oh and Park, 2003).

2.2.4 Attribute Based Access Control (ABAC)

In ABAC (Hu et al., 2014), permissions to access the objects are not directly given to the subject. It uses attributes of the subject (e.g. name, age or role in organization) and attributes of object (e.g. metadata properties) to provide authorizations as shown in Figure 4. The permissions in ABAC depend on a combination of a set of attributes and their relative values (Ubale Swapnaja et al., 2014).

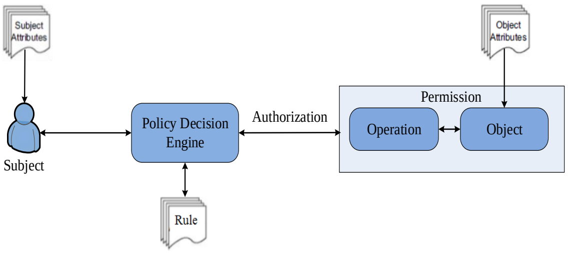


Figure 4: Overview of the ABAC model.

ABAC overcomes the user role assignment problem exist in RBAC and focuses on the attributes of a user requiring to grant access. It is a very flexible model that is considerably easier to administer than RBAC. However, higher flexibility comes with higher complexity due to the specification and maintenance of the policies. The number of subjects and objects in healthcare systems increases dynamically. This requires maintaining database which contains all attributes in same format (Verma et al., 2012).

2.2.5 RBAC Extensions

The strength of RBAC lies in its manageability. It is fairly easy to assign authorization to users based on their roles. Unfortunately, RBAC alone does not suffice to handle various constraints that are required in diverse domains. RBAC has been broadly extended to support diverse domains in data authorization management with various constraints. Extensions include task-role based (Oh and Park, 2003), team-based (Thomas, 1997; Georgiadis et al., 2001), contextual role-based (Motta and Furuie, 2003), context-aware (Koufi and Vassilacopoulos, 2008) and so forth (Tolone et al., 2005). However, these extended models would add additional complexity to healthcare systems because they still face some problems (Moonian et al., 2008). Granularity and manageability are inversely proportional to one another. Higher granularity in security invariably implies more complex management. This is apparent in attribute-based access control (ABAC), which offers higher control or granularity at the expense of lower manageability. On the other hand, role-based access control (RBAC) evidently provides lesser granularity for better manageability. To combine the strengths of both approaches without being hindered by their limitations, bilayer access control (BLAC) has been devised (Alshehri et al., 2013; Alshehri and Raj, 2013). BLAC enforces a two-layer access control that initially applies RBAC and ABAC. The model uses the concept of pseudorole, which is defined as a set of static attributes of subjects. A pseudorole is not a real role, which is traditionally defined as a job function. Subjects' attributes are categorized as static attributes (when attribute values typically do not change) used to generate pseudoroles and dynamic attributes (when attribute values change frequently). Static and dynamic attributes are used in policies to constrain pseudoroles (Alshehri and Raj, 2013).

Despite the advantages offered by BLAC, it is not exclusively tailored for collaborative healthcare system. BLAC focus has not been placed on supporting collaboration and coordination work. Thus, an additional policy can be defined at the 2^{nd} layer of BLAC to ensure more secure interaction between cooperating parties. Although secure collaboration is achievable via intricate policy management, doing this would basically reduce the approach to ABAC. Thus, the issue of low manageability may resurface when using BLAC to secure a collaborative effort.

3 PROPOSED ACCESS CONTROL MODEL

To alleviate the aforementioned limitation of BLAC and satisfy access control requirements for collaborative healthcare systems, work-based access control (WBAC) model is proposed (Figure 5). In the proposed model, a secondary RBAC layer, with extra roles extracted from team work requirement, is added to BLAC to manage the complexity of cooperative engagements in the healthcare domain. Policies related to collaboration and team work are encapsulated within this coordinating layer to ensure that the attribute layer is not overly burdened. The main concepts of our model are:

1. Subjects are assigned to pseudoroles and/or team role (section 3.1) and objects are associated with WBAC policies; main policy and collaboration policy.
2. Access control is performed on three-step evaluation procedure; pseudoroles evaluation, team role evaluation and rule examination (section 3.3).

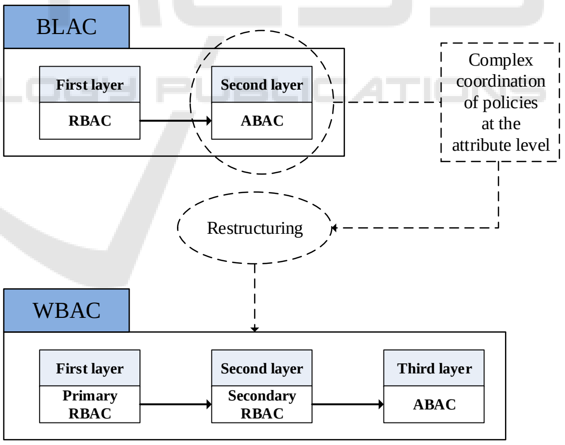


Figure 5: BiLayer Access Control and Work Based Access Control.

In this study, "work" is defined as an entity comprising a collection of elements that interact with one another for a particular outcome to be achieved successfully. As shown in Figure 6, the fundamental idea is that work itself demands completion, and it is directly linked to the patient, context, personnel and goal.

A goal is directly linked to an objective and an objective is broken down into a set of tasks. The difference between a goal and an objective is that, a

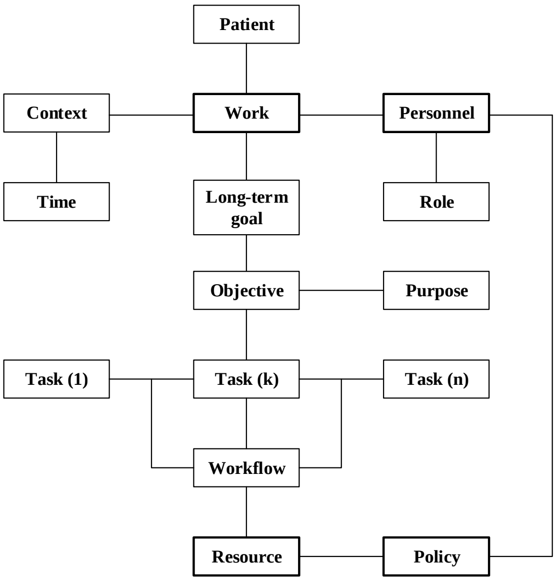


Figure 6: Work Model for Collaboration.

goal consists of long-term aims that need to be accomplished (e.g. treatment of patient) and an objective comprises of concrete attainments that can be achieved by following a certain number of steps. Personnel in the collaboration will have their own roles. In performing a certain task, personnel must access resources that are governed by policies.

3.1 Team Role

Team is defined as a collection of participants in specific role with objective of accomplishing a specific work (Thomas, 1997). Each team has a responsible team manager. Any of the participants joining a team shares a common goal and may share a default set of permissions for their cooperative work. The notion of a team role is used to restrict access permissions to those individuals who not only have the right organizational roles but also are associated to the task via team membership (Wang, 1999).

Regarding the process of collaboration and team work, access control model must be able to provide an efficient and secure platform for people to work together in a hospital without being deterred by restrictive enforcement of access control policies (Le et al., 2012). This can be a rather delicate situation to handle, given the fact that the fluidity of teamwork within the medical domain is often incongruent with technological security. To demonstrate this notion, we consider a scenario (section 1.1) involving four medical practitioners who are working together on a patient's case. For the sake of securing the patient's private (sensitive) data (e.g. mental illness, etc.), the collaboration must be clearly defined. By default, only the main practitioner should be aware of the patient's personal information (need-to-know principle). The three other medical practitioners with supporting roles are given information based on their contributing roles. In order to achieve this, it is imperative to determine the finer roles of each team member. The team role of each member will subsequently determine the extent of access given. For instance, if the supporting party is included solely for consultation purposes concerning the disease, only information essential for diagnosis is provided. It is not necessary to allow perusal of personal information related to the patient. In this way, improper access to the patient's sensitive information can be prevented.

Hospital personnel roles are often simplistically split into medical practitioners, nurses and administrators. However, their roles in a team can be further categorized using the team role theory (Córdoba and Piki, 2012). This theory contends a total of nine roles per group, which are classified into thought, action and management. For the purpose of this research, they are rephrased and illustrated in Figure.7.

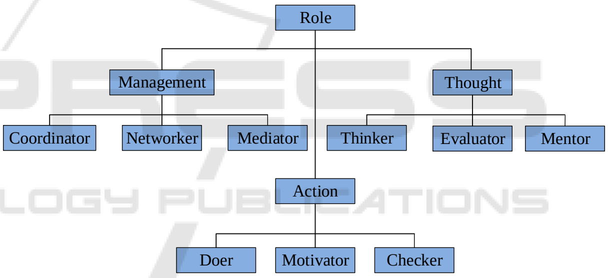


Figure 7: Taxonomy of Team Role.

Thought denotes a role that is dominated mostly by thinking. To be a successful thought collaborator, the person may need to understand the medical predicament in detail without necessarily knowing the patient. A worker in this role could be involved in devising strategies to confront particular medical enigmas. Thus, a cardiology specialist may offer his/her expertise regarding the best practices of performing a heart transplant on a child without being involved in the actual operation.

Action, as the labeling suggests, signifies being involved in task-related collaboration, such as meeting the patient for a medical check-up. Having an action role usually implies close interaction with the patient. Nevertheless, discretion is still feasible with care. For instance, an anesthesiologist needs to only know the patient's physical characteristics to prepare anesthetic. Who the patient is, or where the patient lives is not relevant to completing this task.

The *management* category comprises personnel who are mostly involved in managing others. These types of collaborators are adept at coordinating teamwork that is susceptible to social or psychological challenges. For example, in conflict management, they may have to resolve series of opposing diagnoses made by medical practitioners and that may otherwise escalate into serious altercations. In this regard, such personnel's need for information is inwardly oriented. They have a greater need to know personal information about others working at the hospital rather than of patients.

3.2 Work-Based Access Control

Work-based access control (WBAC) combines the pseudorole in BLAC (section 2.2.5) and team role to enable a multilayered role facility that is driven by collaboration. Merging (Figure 8) is done by simplifying the inherent classification of team roles into four elementary roles, i.e. the main, thought, action and management roles. Here, collaborative team roles are combined with the main role and are placed in the same group. This way, access control is enforced with superior flexibility and it promotes abstraction of the collaborative characterization of access control from the main flow. This ensures more manageable implementation as a whole. Process wise, the original BLAC procedure is enhanced with an added decision mechanism that provides an alternative route for parties beyond the normally established policy.

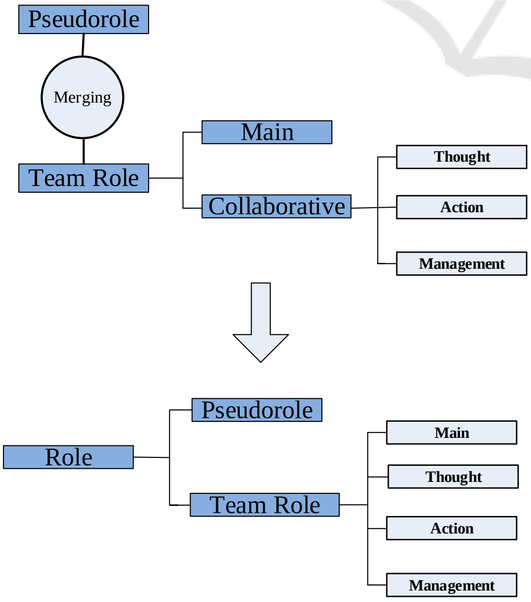
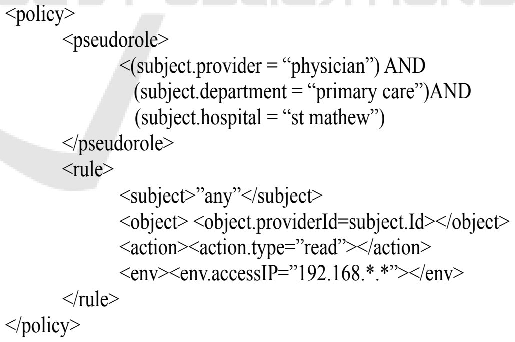


Figure 8: Merging of Pseudorole and Team Role.

Multiple role layers (Wen et al., 2009) segregate access validation into two modes. Verification is done sequentially, whereby normal validation in BLAC gains precedence over WBAC. In other words, the pseudorole is validated first, followed by team role validation. Separating the roles is a delicate agenda as the integrity of access control during collaboration must be guaranteed.

consider the following scenario to appreciate the limitation of BLAC in managing problems potentially arising with regard to collaborative work. Suppose a physician from the primary care unit requires the help of another physician from the oncology department. In the policy prior to collaboration (Figure 9), only the physician in the primary care department has access to reading the object or resource. Therefore, any access request by the oncology department physician would be denied.

The policy defined in Figure 9 can be visualized better by studying the decision logic and process in BLAC (Figure 10). The access decision engine always checks the pseudorole's validity first. The physician from the oncology department would have to pass the initial validation for being a physician. However, when the engine discovers that the physician's department is not primary care, access consideration halts immediately. In order to solve this problem, BLAC recommends a modification to the original policy. A possible modification that allows an oncology department physician to read data created by the main, primary care physician, is shown in Figure 11.



```
<policy>
        <pseudorole>
                <(subject.provider = “physician”) AND
                  (subject.department = “primary care”)AND
                  (subject.hospital = “st mathew”)
        </pseudorole>
        <rule>
                <subject>”any”</subject>
                <object> <object.providerId=subject.Id></object>
                <action><action.type=”read”></action>
                <env><env.accessIP=”192.168.*.*”></env>
        </rule>
</policy>
```

Figure 9: Original Policy Prior to Collaboration.

At first glance, the policy seems valid. It now offers access to a new department called oncology. Enabling proper access to the object based on the collaborator's subject ID is somewhat complicated. It is difficult to define the implications of collaboration on the rule itself because it is structured by subject, object, action and environment. Therefore, a new attribute is introduced known as the ’collaboratorId’. This new collaboratorId attribute should be enforced only on two conditions: the objects are created by the physician and are necessary for collaboration. However,

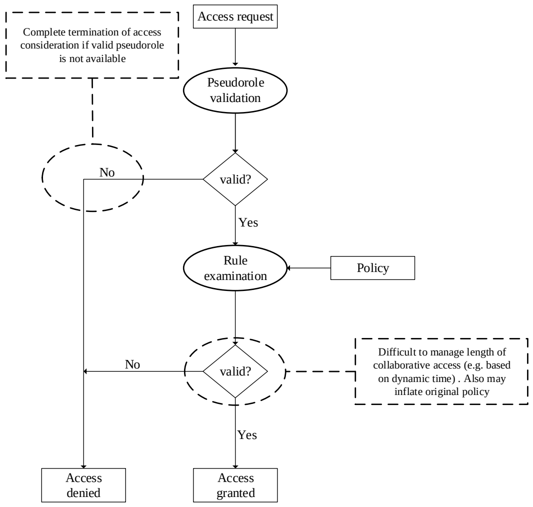
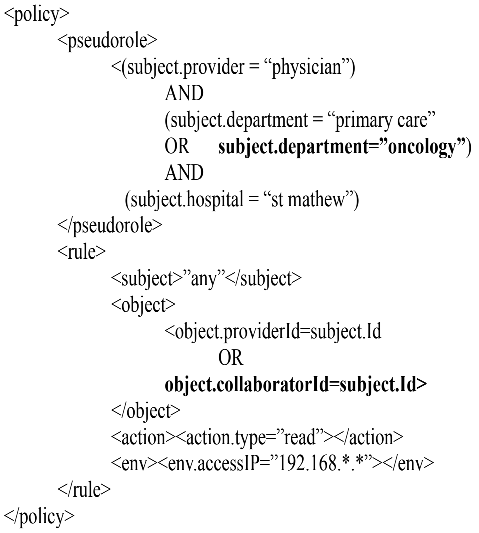

Access request
Complete termination of access consideration if valid pseudorole is not available
Pseudorole validation
valid?
No
Yes
Rule examination
Policy
valid?
No
Difficult to manage length of collaborative access (e.g. based on dynamic time) . Also may inflate original policy
Yes
Access denied
Access granted

Figure 10: Flow of BLAC for Invalid Pseudorole.

this is a rather tedious process because it involves the additional task of security management. For convenience, suppose that all objects created by the physician in the primary care department are updated with the collaboratorId. Updating the objects with collaboratorId implies that the oncology department physician can now read every object created by the former physician. This is true regardless of each one's purpose in the collaboration. Thus, if a confidential object is created by the primary care physician for the purpose of a crime investigation, it is visible to the collaborating oncology physician as well.

Apart from difficulty controlling the scope of access, employing BLAC for collaboration can also be a source of additional complexity in constructing the rules of a policy. It is worth noting that the modification requires two changes. The first change is done to the pseudorole and the second to the object of the rule, which is not desirable. It is better to minimize the changes.

In addition to the aforementioned dilemmas, another issue must be addressed. Controlling the length of collaboration is also a cumbersome endeavor. For instance, in limiting the collaborating party's access based on the time factor, the rules must be modified intricately since time is fundamentally dynamic. If not performed with care, access could be temporally extended beyond necessity. Given the constraints faced by BLAC in managing collaborative access control implementation, a more dynamic policy with dual inclination is proposed as shown in Figure 12, whereby the normal policy of enforcing access control is contained within the main policy. On the other hand, any policy that mediates resource sharing is covered by the collaboration policy. This way, better access control management is achievable.



```
<policy>
    <pseudorole>
        <(subject.provider = "physician")
            AND
            (subject.department = "primary care"
            OR    subject.department="oncology")
            AND
          (subject.hospital = "st mathew")
    </pseudorole>
    <rule>
        <subject>"any"</subject>
        <object>
            <object.providerId=subject.Id
                OR
            object.collaboratorId=subject.Id>
        </object>
        <action><action.type="read"></action>
        <env><env.accessIP="192.168.*.*"></env>
    </rule>
</policy>
```

Figure 11: Modified Policy Due to Collaboration.

Certain concerns may arise with a dual policy in the access control model, the most apparent of which would be priority. For instance, in situations where one policy opposes the other, which would dominate? It is therefore clearly defined that when two policies are in conflict, the main policy is always given the highest priority, regardless of context.

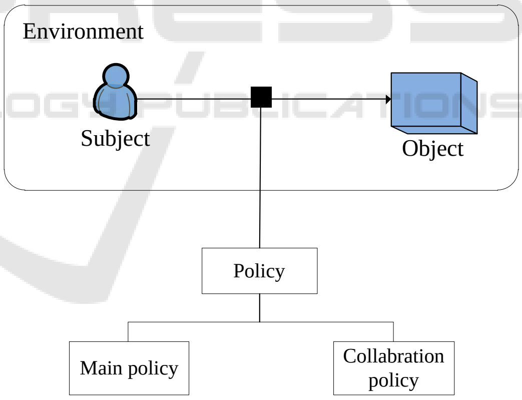


Figure 12: Dual Policy in WBAC.

3.3 Flow model of WBAC

Similar to the core process of BLAC, access request in WBAC first undergoes pseudorole validation as shown in Figure 13. At this stage, the user's pseudorole is compared against the one defined in the policy. In BLAC, failing this step results in the complete termination of decision logic. WBAC, however, treats this differently. If the request fails, the resource is inspected further to determine whether it is part of collaborative work. If it is, then the team role of the user in question is properly extracted and examined.

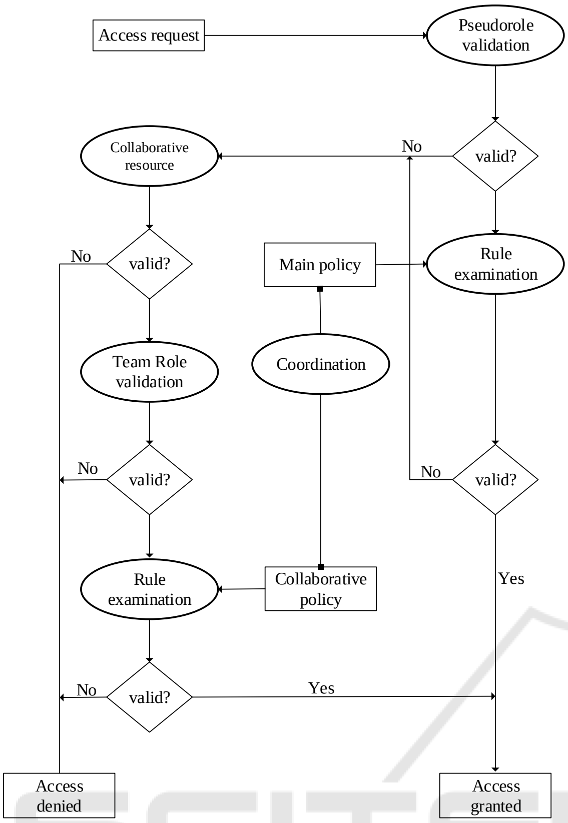


Figure 13: Flow of WBAC.

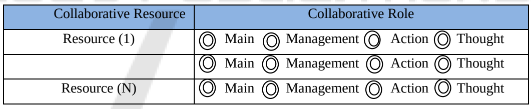
In cases where the user possesses a valid team role over the resource, the extent of access is determined by the collaborative policy. This policy controls the granting of access according to the user's purpose within the team. For instance, users with the action team role receive more access to a patient's personal information as compared to users with the management team role. This is because the former type of user is in greater need of the information to perform their job than the latter.

Complications might arise in terms of coordinating the ramification of two different policies, i.e. the main and collaborative policies. Considerable concern would also pertain to whether a request initially denied by the main flow should be granted access by an alternative flow. In resolving this, it must be noted that the nature of collaboration is never free from risk. Sharing information always entails compromise to certain parts of security. As such, it is impossible to negate the danger altogether.

As mentioned in earlier sections 2.1, a realistic way of handling collaboration risk is to minimize the discrepancy between the granted and the required access. This is where the coordination element becomes vital. The delimiting principle of access restriction must be balanced with the necessity for information distribution. Excessive restriction can hamper cooperation while too much freedom can entirely defeat the purpose of security.

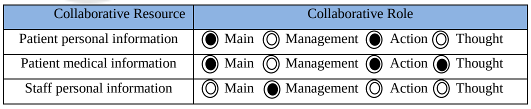
A way of simplifying conflict resolution between competing policies is to utilize a tabular representation in organizing shared resources and team roles. Each resource contains four options that reflect the team role involved. The options should not be exclusive by nature and the administrator can select none or all. Zero selection implies that the resource is not open to collaborative access and can only be accessed based on user-related pseudoroles and rules. In contrast, complete selection means the resource is publicly available to everyone collaborating.

To concretize the possibility of using tabularization in defining a collaboration policy, it would be useful to consider the illustration below (Figure 14). Here, the collaborative resources required for work are enumerated in table form. Each shared resource is tied to the set of collaborative roles or team roles that can access it. In effect, the selected roles will determine the extent of collaborative access. Note that the collaborative role for a particular resource should be set in accordance with its purpose (Figure 15). A patient's personal information is vital to the main collaborator and those with an action team role. However, medical information, which might be less sensitive and fundamental to treatment than personal information, should be made accessible to most team roles except the people role.



Collaborative Resource	Collaborative Role
Resource (1)	○ Main ○ Management ○ Action ○ Thought
	○ Main ○ Management ○ Action ○ Thought
Resource (N)	○ Main ○ Management ○ Action ○ Thought

Figure 14: Simplification of Collaborative Role into Tabular Form.



Collaborative Resource	Collaborative Role
Patient personal information	● Main ○ Management ● Action ○ Thought
Patient medical information	● Main ○ Management ● Action ● Thought
Staff personal information	○ Main ● Management ○ Action ○ Thought

Figure 15: Collaborative Resource and RoleC.

4 CONCLUSIONS AND FUTURE WORK

In this work, an access control model was proposed that is suitable for collaborative healthcare systems to address the issue of information sharing and information security. The aim is to provide a flexible access control model without compromising the granularity of access rights. The major contributions of this work are as follows. First, the proposed model offers fine-grained control of access rights granting. Healthcare providers are granted access only to the specific resource (patient records) instances that are bound to work task execution. Secondly, WBAC corresponds to the least privilege principle, whereby healthcare providers are granted minimal access rights for carrying out duties, or tasks. Third, the WBAC model ensures that access rights are dynamically adapted to the actual needs of healthcare providers. Healthcare providers can access the resources associated with a work task, but only while the work task is active. Once the work is completed the access rights are invalidated.

4.1 Verification and Validation

The WBAC scheme will be further investigated at the ”Center for eHealth and Health Care Technology” at the University of Agder. The plan is to formalize the proposed event and policy, develop and prototype the functionality to be implemented as well as evaluate the validity of the model. In order to evaluate the model's validity, three main dimensions are evaluated: security, efficiency and practicality. Security refers to the model's capacity to facilitate confidentiality and integrity in healthcare systems. Practicality denotes the possible difficulties in managing the model during actual implementation. Finally, efficiency is the model's performance in terms of resource consumption, e.g. time. Moreover, the problems of inconsistency and incompleteness (Shaikh et al., 2010; Aqib and Shaikh, 2014) of the access control policy set will be validated and verified.

Formal specification and verification of WBAC policies is important. We consider using linear temporal logic (LTL) (Rozier, 2011) as formalism for specifying WBAC policies. LTL allows a convenient and concise formalism for specific policies as well as used for verifying properties of reactive systems. In additions, NIST's (National Institute of Standards and Technology) generic model checking technique (ACPT (Access Control Policy Testing)) (Hwang et al., 2010) will be used to model and verify policies during policy modeling to assures that WBAC policies satisfy the security properties intended by the model.

Use of formal methods, while important, cannot verify usefulness and properties that are not captured within the model and the formalism. We therefore see formal verification as a necessary, but not sufficient, condition for validation of WBAC in eHealth scenarios.

The plan is also to analyze the insider threat in the domain of healthcare information sharing and examine whether WBAC will perform effectively and efficiently on identified threats. Furthermore, access control policies, compliance and human factors will be considered. The access control policies need to be shaped and evaluated in term of their human impact (Probst et al., 2010). The idea is how to define a set of consistent access control policies related to human behaviors, and fit it to healthcare processes and the way people work, including in emergency situations.

ACKNOWLEDGEMENTS

We would like to thank the ”Center for eHealth and Health Care Technology” at the University of Agder for the support in investigating WBAC.

REFERENCES

Alhaqbani, B. and Fidge, C. (2008). Access control requirements for processing electronic health records. In *Business Process Management Workshops*, pages 371–382. Springer.

Alotaiby, F. T. and Chen, J. X. (2004). A model for team-based access control (tmac 2004). In *Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on*, volume 1, pages 450–454. IEEE.

Alshehri, S., Mishra, S., and Raj, R. (2013). Insider threat mitigation and access control in healthcare systems.

Alshehri, S. and Raj, R. K. (2013). Secure access control for health information sharing systems. In *Healthcare Informatics (ICHI), 2013 IEEE International Conference on*, pages 277–286. IEEE.

Aqib, M. and Shaikh, R. A. (2014). Analysis and comparison of access control policies validation mechanisms. *International Journal of Computer Network and Information Security (IJCNIS)*, 7(1):54.

Córdoba, J.-R. and Piki, A. (2012). Facilitating project management education through groups as systems. *International Journal of Project Management*, 30(1):83–93.

Fabian, B., Ermakova, T., and Junghanns, P. (2015). Collaborative and secure sharing of healthcare data in multi-clouds. *Information Systems*, 48:132–150.

Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., and Chandramouli, R. (2001). Proposed nist standard for role-based access control. *ACM Transactions on Information and System Security (TISSEC)*, 4(3):224–274.

Ferreira, A., Ricardo, C.-C., Antunes, L., and Chadwick, D. (2007). Access control: how can it improve patients healthcare? *Medical and Care Compunetics 4*, 4:65.

Gajanayake, R., Iannella, R., and Sahama, T. (2014). Privacy oriented access control for electronic health records. *electronic Journal of Health Informatics*, 8(2):15.

Georgiadis, C. K., Mavridis, I., Pangalos, G., and Thomas, R. K. (2001). Flexible team-based access control using contexts. In *Proceedings of the sixth ACM symposium on Access control models and technologies*, pages 21–27. ACM.

Hu, V. C., Ferraiolo, D., and Kuhn, D. R. (2006). *Assessment of access control systems*. US Department of Commerce, National Institute of Standards and Technology.

Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., and Scarfone, K. (2014). Guide to attribute based access control (abac) definition and considerations. *NIST Special Publication*, 800:162.

Hwang, J., Xie, T., Hu, V., and Altunay, M. (2010). Acpt: A tool for modeling and verifying access control policies. In *Policies for Distributed Systems and Networks (POLICY), 2010 IEEE International Symposium on*, pages 40–43. IEEE.

Kayem, A. V., Akl, S. G., and Martin, P. (2010). *Adaptive cryptographic access control*, volume 48. Springer Science & Business Media.

Koufi, V. and Vassilacopoulos, G. (2008). Context-aware access control for pervasive access to process-based healthcare systems. *Studies in health technology and informatics*, 136:679.

Le, X. H., Doll, T., Barbosu, M., Luque, A., and Wang, D. (2012). An enhancement of the role-based access control model to facilitate information access management in context of team collaboration and workflow. *Journal of biomedical informatics*, 45(6):1084–1107.

Majumder, A., Namasudra, S., and Nath, S. (2014). Taxonomy and classification of access control models for cloud environments. In *Continued Rise of the Cloud*, pages 23–53. Springer.

Moonian, O., Cheerkoot-Jalim, S., Nagowah, S. D., Khedo, K. K., Doomun, R., and Cadersaib, Z. (2008). Hcrbac–an access control system for collaborative context-aware healthcare services in mauritius. *Journal of Health Informatics in Developing Countries*, 2(2).

Motta, G. H. and Furuie, S. S. (2003). A contextual role-based access control authorization model for electronic patient record. *Information Technology in Biomedicine, IEEE Transactions on*, 7(3):202–207.

Oh, S. and Park, S. (2003). Task–role-based access control model. *Information systems*, 28(6):533–562.

Probst, C. W., Hunker, J., Gollmann, D., and Bishop, M. (2010). *Insider Threats in Cyber Security*, volume 49. Springer Science & Business Media.

Rozier, K. Y. (2011). Linear temporal logic symbolic model checking. *Computer Science Review*, 5(2):163–203.

Rubio-Medrano, C. E., D'Souza, C., and Ahn, G.-J. (2013). Supporting secure collaborations with attribute-based access control. In *Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom), 2013 9th International Conference Conference on*, pages 525–530. IEEE.

Russello, G., Dong, C., and Dulay, N. (2008). A workflow-based access control framework for e-health applications. In *AINAW 2008-Workshops. 22nd International Conference on*, pages 111–120. IEEE.

Samarati, P. and Di Vimercati, S. D. C. (2001). Access control: Policies, models, and mechanisms. *Lecture notes in computer science*, pages 137–196.

Shaikh, R. A., Adi, K., Logrippo, L., and Mankovski, S. (2010). Inconsistency detection method for access control policies. In *Information Assurance and Security (IAS), 2010 Sixth International Conference on*, pages 204–209. IEEE.

Shen, H. and Dewan, P. (1992). Access control for collaborative environments. In *Proceedings of the 1992 ACM conference on Computer-supported cooperative work*, pages 51–58. ACM.

Thomas, R. K. (1997). Team-based access control (tmac): a primitive for applying role-based access controls in collaborative environments. In *Proceedings of the second ACM workshop on Role-based access control*, pages 13–19. ACM.

Tolone, W., Ahn, G.-J., Pai, T., and Hong, S.-P. (2005). Access control in collaborative systems. *ACM Computing Surveys (CSUR)*, 37(1):29–41.

Ubale Swapnaja, A., Modani Dattatray, G., and Apte Sulabha, S. (2014). Analysis of dac mac rbac access control based models for security. *International Journal of Computer Applications*, 104(5).

Verma, S., Kumar, S., and Singh, M. (2012). Comparative analysis of role base and attribute base access control model in semantic web. *International Journal of Computer Applications*, 46(18).

Wang, W. (1999). Team-and-role-based organizational context and access control for cooperative hypermedia environments. In *Proceedings of the tenth ACM Conference on Hypertext and hypermedia: returning to our diverse roots: returning to our diverse roots*, pages 37–46. ACM.

Wen, Z., Zhou, B., and Wu, D. (2009). Three-layers role-based access control framework in large financial web systems. In *Computational Intelligence and Software Engineering, 2009. CiSE 2009. International Conference on*, pages 1–4. IEEE.

Zhang, R. and Liu, L. (2010). Security models and requirements for healthcare application clouds. In *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, pages 268–275. IEEE.