An Access Control Model for easy management of patient privacy in EHR systems

Mario Sicuranza
Institute for High Performance Computing and Networking
of the Italian National Research Council (ICAR-CNR)
Via Pietro Castellino, 111 – 80131 Napoli – Italy
mario.sicuranza@na.icar.cnr.it

Angelo Esposito
Institute for High Performance Computing and Networking
of the Italian National Research Council (ICAR-CNR)
Via Pietro Castellino, 111 – 80131 Napoli – Italy
angelo.esposito@na.icar.cnr.it

Abstract — **In EHR systems most of the data are confidential concerning the health of a patient, so it is necessary to provide a mechanism for access control. This has to ensure not only the confidentiality and integrity of the data, but also to allow the definition of security policies which reflect the need for privacy of the health care organization that manages the data; of the patient, who the documents refer to; and finally of international and national directives and norms. In literature there are several access control models, each of which responds just partially to the need for patient privacy. In this paper an innovative access control model is defined. It meets the main features that have to be satisfied by an EHR. Our proposal is an advanced access control model that combines several access control models known in the literature. It adds the characteristics of modularity and easiness in the management of access policies, focusing attention on privacy and patient's consent (patient privacy centric). The model provides the ability to define and to realize fine-grained access policies, which can be defined independently by both healthcare organizations and by patients. Our model is Attribute-based, multi-level, modular and with a dynamic and temporal management of the users' lists.**

Keywords: Access control model; privacy; EHR; patient consent; patient centric.

I. INTRODUCTION

Electronic Health Record (EHR) systems enable the collection and sharing of electronic clinical data among different healthcare organizations. An EHR system provides a variety of services to manage data, and also a certain number of high-level services that reduce medical errors and improve the quality of care. Iakovidis [1] defined an Electronic Health Record as "digitally stored healthcare information about an individual's lifetime with the purpose of supporting continuity of care, education and research, and ensuring confidentiality at all times". The core of the EHR system is represented by the patients' clinical data and the ability to access and to use these data. Clinical data on EHR systems are characterized by sensitive information, so they should be protected from unauthorized access. So for EHR systems it is necessary to ensure the confidentiality of data and patient's privacy, and to guarantee the quality of the data and the integrity that leads the user (doctor) to have confidence in the data and in the information contained. To meet these (integrity, confidentiality, and quality) needs a widely used mechanism is Access Control (AC), which is a fundamental security barrier for securing data in a healthcare information system. The AC is a mechanism that limits who can access the documents in an EHR system and how they can operate them. In the literature there are several models of access control, each one with different characteristics but all with the common goal of protecting data from unauthorized access. EHR systems should allow the definition of security policies (via the AC model) which reflect the following needs : i) of the health care organization that manages the data; ii) of the patient; and iii) especially of the law and the directives in terms of the protection of medical data and patient's consent.

In literature, there are different access control models, such as Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC), starting from which more sophisticated models, closer to the needs for privacy, were later defined, such as the Privacy-aware Role Based Access Control Model (P-RBAC) and the Purpose-Based Access Control Model (P-BAC).

Each of these responds just partially to patients' needs for privacy, as most of them have limitations in the possibility of accurate and flexible management of the security policies. On the contrary the aim of our model is to obtain the maximum accordance between what the access policies allow us to define and what the patients want to define.

In addition, an EHR is typically a distributed and heterogeneous system [16]. In fact, it is composed of different and autonomous healthcare organizations, each of which can express its own security policies, independently of the others. Therefore, it is necessary to define an AC model that provides high flexibility in the management of the access policies.

In contrast to the models known in the literature, we define an AC model with characteristics of modularity, flexibility and fine-grained specification in the definition of policies and dynamism in their management.

Another feature of the proposed model is that it is patient privacy-centric, that is, there is the possibility to define fine-grained policies in compliance with the patients' needs for privacy, which can be expressed through their consent to healthcare organizations or directly by the patients themselves.

Our solution is an advanced access control model that combines several AC solutions known in the literature, extending to them the characteristics of easiness in the management of access policies, and focusing attention on

privacy and patients' consent (patient privacy centric). The obtained model is Attribute-based, multilevel, modular and with a dynamic and temporal management of the users' lists (through which it is possible to specify authorized users on the system). The paper is organized as follows. Section II contains the related work regarding AC models. Section III illustrates some healthcare access control requirements for EHR systems. In Section IV our model is presented. In Section V an algorithm for the AC that uses our model is shown. Section VI shows a possible scenario that highlights the peculiarities of the MPP-ABAC model. Section VII concludes the paper and outlines future work.

II. RELETED WORK

In this section we briefly survey related work about Access Control Models. In 1969, in the work of Lampson [2], a formal definition of access control is given. This first model has a set of subjects and objects and it associates to each couple of subjects/objects the list of possible operations. In time different models have been presented. In 1975, the first multilevel model was presented by Bell-LaPadula [3]. Such a model consists of four access levels and access labels, that are un-classified, confidential, secret, and top secret. Later the Discretionary Access Control (DAC) and Mandatory Access Control (MAC) models were defined, that today have become two traditional access models, from which almost all the others arise. The DAC model allows the user, the owner of the resources, to grant or deny access to the resources to other users, first through the definition of an Access Control Matrix, then via an Access Control List. The MAC model is derived directly from the model of Bell-LaPadula. In fact, as in the model [4], in the MAC Model every subject and every resource has a security level. The MAC defines access rules between subject levels and resource levels, typical rules being *Read Down* and *Write up* to ensure the privacy, and *Read Up* and *Write Down* to guarantee integrity. Later, Ferraiolo and Kuhn [5] defined a first Role Based Access Control (RBAC) model, using, in a different way, the concepts of users, operations and groups and defining the concept of role. In this way, a more streamlined management of the policies in an enterprise system is allowed. Many RBAC models, that were realized subsequently, introduce the concept of hierarchy and a partial order among the different roles, which allows a further simplification in the management of policies. An extension of the RBAC model is the Temporal Role-Based Access Control Model (TRBAC) [6], which allows a temporal enabling and disabling of the role. Another very flexible model is Attribute Based Access Control (ABAC) [7], which introduces the attributes associated with roles in order to add further constraints to the separation of duty [6]. In the last few years different AC models have been proposed, which aim at satisfying the needs for the protection and privacy of sensitive data. For example, the Hierarchical Privacy-Sensitive Filtering (HPSF model) [8] has been defined for the protection of data on relational databases, with the definition of privacy levels for the data. The owner of given data specifies its privacy-sensitive level (PLS). Moreover, every user in the system is associated to an user privacy-sensitive level (UPSL). The access to data is regulated as in the multi-level security models, the access, in fact, depending on the compatibility between PSL and UPSL. A further model, which focuses on the need for definitions of policy related to the requirements of patient privacy, is the Privacy-Aware Role Based Access Control (P-RBAC) [9]. This model is an extension of the RBAC model, in which not only the role and the permissions, that such a role has on the required object, are considered, but also the purpose of the access to the object and the defined privacy policies in compliance with the user's will. Finally, the Purposed-Based Access Control Model (P-BAC) [10] introduces the hierarchical notion purposed in the model. In fact, the roles and the operations are classified in a hierarchical manner according to the purpose. The access policy is defined comparing the hierarchy level of the role to the level of the requested operation. All these models present some limitations in the use of EHR systems. For example, the data in the EHR system are mostly clinical documents, and for this reason it is not easy to identify the owner of the document. There are several subjects, such as the author of the document, the holder of the document and the patient, that could be considered the owner of the document, depending on the point of view. Therefore, the DAC model cannot be the only one used to manage the access policies to the EHR system. In the DAC model, the owner of the data stored in the EHR is identified. Furthermore, the DAC model is not scalable in a system of large dimensions, because it requires the definition of a matrix (user/ objects /operations), which is, in this case, a complicated management. Instead, in the MAC model security labels are associated to resources. It is difficult to use only this model in EHR systems because a given document could be characterized by different security levels depending on the patient or on the healthcare organization responsible for the data. This model is devoid of the flexibility necessary to be used alone for an EHR system. The RBAC model is static, since the association among roles, operations and objects is made upstream and it is defined by the system. The RBAC model is characterized by a greater flexibility compared to the MAC model and it is easier to handle compared to the DAC model, but it still has many limitations on its use in an EHR system, such as the need to define common and shared roles for healthcare organizations and the lack of flexibility and dynamicity, that is the possibility of policy management by the patients, who in this model cannot change these repeatedly. In fact, to have more flexibility, the attribute-based access control model has been introduced, in which additional attributes associated with the role are used. In privacy-aware role based access control and purposed-based access models, the purpose attribute plays a key role in ensuring also the privacy of the patient. Although many of the latest models allow you to ensure the needs of the EHR system, they still lack components for dynamicity, which leads the patient not to have a full and easy control of his privacy. For these reasons, the model that we will present aims to overcome the limitations of the static nature in policy management, since the flexibility in the definition of policies is a fundamental requirement in an EHR system. The model combines particular features derived from several models in the literature and it realizes the characteristic of flexibility by introducing the concepts of Purpose, Roles and Users List. It also gives the patient full power in the definition of privacy policies in complete accordance with the consent he wants to provide to her/his clinical documents. The definition

of the model is obtained starting from identifying the basic requirements to use it in an EHR system. In the next section the different requirements are presented.

III. Requirements of Healthcare Access Control

In the previous section we have described some AC models, then illustrating the limitations of their use in EHR systems. In this section we identify the main features that an access control model for an EHR system must satisfy. A suitable model for EHR systems should meet at least a set of requirements arising from: i) the patient who the documents refer to; ii) the healthcare organizations holding the data, and iii) the international, national and local directives and norms.

A. Requirements of Patients

The patients' needs are related to the confidentiality of their data in the EHR systems. Patients should trust the system and they should be able to specify the level of privacy they want to associate to their documents.

- P1. Patients should have the right of control over their own clinical documents. They must be able to specify who can do what on their own documents;
- P2. Patients should have the ability to change at any time the rights of access to their documents;
- P3. Patients must be able to hide their documents from specific healthcare practitioners;
- P4. Patients need to have the ability to see how and when their documents are accessed by the users who have access rights on them and for which purpose. This will be possible through the property of Disclosure, which is indicated in the EU directives. The patients should be able to provide access to healthcare practitioners that are not entitled to access the patients' documents.

B. Requirements of Healthcare organizations

Healthcare organizations must provide protection to the data they hold. Every healthcare organization can manage security policies with a certain level of autonomy.

- H1. Every healthcare organization should be able to design its own security policy and to enforce it. The definition of the access policies must be implemented in total freedom and through a highly flexible mechanism;
- H2. The healthcare organizations should be able to change quickly and easily the access policies of a given document.
- H3. The Access control should not add a significant administrative overhead.

C. Requirements arising from International Norms and Directives

In 2012 the European Commission unveiled a draft European General Data Protection Regulation based on the following properties and principles:

- D1. Informed Consent, every processing of personal data will require the provision to the concerned individuals of clear and simple information, as well as obtaining specific and explicit consent. Users must be informed about what happens with their data, and they must be able to agree consciously to the processing of the data. This property corresponds to the 4th property (P4) mentioned above;
- D2. The property of "Right to be forgotten", with which a patient is able to delete the history of his documents;
- D3. The property of Purpose, whereby the data must be used for the indicated purposes;
- D4. The property of Disclosure, which suggests that patients should know how their data are used;
- D5. The management of access control must be easy to access in case a document is accessed for emergency purposes.

Table 2 in the next section shows how the listed requirements are satisfied in our model.

IV. Proposed Access Control Model

This section presents the AC model for an EHR System that allows the satisfaction of the requirements listed in the previous section. Table 2 summarizes how the requirements are satisfied, showing the several model components.

The AC model, as said before, is patient privacy-centric. By "patient privacy-centric" we mean the ability of the model to provide a security policy management, which is based on the patient's will. Such will can be expressed either by the patient's consent indicated by the healthcare organization when a document is inserted in the EHR system, or directly by the patient who operates on the system (for example through the GUI). In this way, she/he will be able to define, in a dynamic manner, the policies depending on her/his privacy needs. Our model extends the RBAC model with further components, in order to obtain a multilevel and attribute-based solution with a dynamic management of the policies. It is attribute-based, in the sense that it grants or denies access to certain operations depending not only on the role (as in the RBAC model), but also on other attributes. In our case, the attribute *Purpose* is particularly relevant, in that it indicates the intent of access to the document, and it allows us to satisfy patient privacy needs, as we will show below. Furthermore, our model is multilevel, because it consists of multiple control levels (such as in the Bell-LaPadula model [4]). The management of the policies in our proposed model is dynamic, in the sense that the model allows us to define easily and rapidly the policies based on the patient's will, that can change in time. We have realized the structure of the model in various steps, using several components of other AC models known in literature. Our model is modular for this reason In figure 1 the different model components and the relationships between them are shown: the components introduced in our model are colored, the others are taken from the RBAC standard model [11].

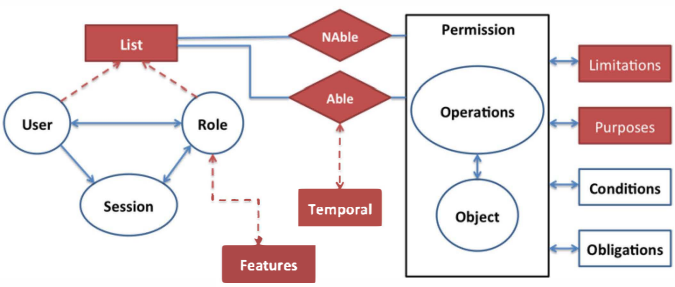

Figure 1. MPP-RBAC model. It contains the components of the presented model.

The fundamental components of our model are:

- The **Temporal** component which allows the management of access rights depending on the time condition, as in the Temporal Model-Based Access Control [6].
- The **Permission** component (RBAC model) which allows the specification of the access rights; that is, it defines which operations are permitted on various objects.
- The **List** relation. It is possible to indicate the association between system users and permissions on objects by means of the **List** relation (*Able* and *Nable*). Therefore, this enables the model to indicate easily the users who have the right to operate on the objects and those who do not have this right.
- The **Purposes** component which associates the Intended Purposes (it is the aim for which a particular document has been collected) to objects, with the goal of limiting document access to the listed purposes only.

Using our model and the **Purposes**, **Limitations** and **Features** components, healthcare organizations can easily and flexibly define and manage access policies in compliance with the consent expressed by the patient. With our model the patient is able to express which system users can access his/her documents and those who cannot for every one of his documents. This is possible through the components **List**, **Temporal**, **Purposes**, the relationships *NAble* and *Able*, and the support functionalities of the model (presented in Section VI). We call the presented model Multi-level-Patient Privacy-centric-ABAC (PP-ABAC). We describe the model in three steps in order to highlight its modular character and to facilitate comprehension.

Step 1 M-RBAC (Multi Level-RBAC)

The model in the first step is a kind of Multi Level RBAC model (M-RBAC), in the sense that it permits us to indicate security levels as in the model MAC. Moreover, one of its levels operates as an RBAC model, obtaining a fusion between the MAC and RBAC models. The modularity of the model provides the ability first (for example at the time of the submission of a new clinical document) to select one of the predefined levels of privacy for the document, such as *top-secret*, *secret*, and *normal*, just as in the MAC model. Each security level has a well-defined security policy, which is set a priori by the healthcare organization. For example, the *top-secret* level might allow access only to the patient and to the author of the document, the *secret* level might allow access to the patient, to the author of document and to General Practitioners. The *normal* level instead could have controls as in the RBAC model. In fact through this model it is possible to associate operations on objects to roles set by the healthcare organization. The level of security associated with the document depends on the patient and on consent that she/he has provided. The choice of the model MAC + RBAC allows a management that is very easy, it in fact being sufficient to indicate the security level based on the fundamental privacy needs of the patient.

Step 2 MP-RBAC (Multi Level P-RBAC)

In the case of the level of privacy being *normal*, it is possible to extend the model obtained in step 1 adding further features to the RBAC model. The first component that we propose to add is the **Purposes** component, which used in the model allows a more fine-grained management of patient privacy (than the RBAC model) through the security policies. It also allows a faster use of the system in the case of access in *Emergency* mode (Access Purpose = Emergency) through the use of the **Features** component, which allows us to associate particular attributes to the roles (for more details see the section "Main algorithm").

The attributes associated to roles are specified in the **Features** component, and are used in the operation of access control. For example, it is possible to associate to a particular role the feature of having access in the emergency mode. This component allows an independent management of emergency policies in healthcare organizations. Through the components introduced at the second step, we obtain a model that is very similar to the P-BAC model [10]. In fact, we have introduced into our model the concepts of *Intended Purpose* and *Access Purpose*, as well as *Hierarchy of Purposes. Intended Purpose* is the aim for which a particular document has been collected. *Access Purposes* is the aim for which a document is requested. In this way a list of *Intended Purposes* is associated to every document, so when a user tries to access a document, the AC evaluates whether a certain *Access Purpose* is compatible with the list of *Intended Purposes*.

The model resulting at the end of the second step is the *Multi Level P-RBAC*.

Step 3 MPP-ABAC (M-Patient Privacy-centric-ABAC)

In step 2 we obtained a fine-grained access model in compliance with the main security needs of EHR systems. In modern EHR systems, as said before, it is necessary to give directly to the patient the opportunity to manage the policies regarding the access to his documents (this is the reason why we define our model as patient privacy-centric). In fact, the European directives (General Data Protection Regulation [12]) move in this direction. To render the management of the access policies easier for the patient, we join other components to the model specified in step 2.

Through these components, the patient can define her/his own policies easily and dynamically, allowing or denying access to her/his documents to specified roles/users and for given purposes. The patient privacy-centric characteristic is introduced into the model through the definition of the components: **Purposes, List**, **Temporal** and **Limitations** and through the introduction of an additional functionality for a dynamic management of document access. In fact, the patient, for every one of her/his documents, can choose the purposes, which are predefined in the system, that she/he wants to associate to her/his documents.

The **List** component enables a dynamic managing of the users and the roles by the patient. It allows a definition of the list of

users and/or roles associated with the **Permission**. In this way it is possible to specify which users have and which ones do not have permission to access through the definition of the relationships *Able* and *NAble*. The relations between **List**, **Temporal** and **Permission** are shown in Figure 1. Furthermore, the **List** component can be used to create a list of the patient's family members, obtaining in this way a management of the system very similar to the Personal Health Record (PHR) system [13].

Through the **Temporal** component, associated with the **List**, the temporal ability as well as dynamic management of this list is provided, for example, in the case of a patient wanting to grant the access to a given document to a specified medical specialist just for a limited time period. Another component added in our model is the **Limitation**, which provides the ability (for example, for a healthcare organization, owner of the documents) to indicate restrictions in the relations Purpose-Permission and List-Permission. For example, in the first association (Purpose-Permission) it could be useful to indicate limitations to the patient adding specific purposes to a given document (for example adding the research purpose on an e-prescription). Through the second association (List-Permission) the healthcare organization (owner of the health document) can restrict access to documents to some roles or subjects. The component **Limitation** allows a minimizing of conflicts among different policies at run-time, allowing at the same time the healthcare organizations to have a supervision of the policies defined by patients. Table 1 illustrates the models used for the definition of our model MPP-ABAC.

Security level	1 Step	2 Step	3 Step
Top-secret	MAC	MAC	MAC
Secret	MAC	MAC	MAC
Normal	RBAC	P-RBAC	PP-ABAC

Table 1. Access models resulting at the various steps

Requirements	Model components
H1	List, Purposes
H2	List, Purposes
H3	MAC components
P1	List, Purposes, Temporal
P2	List, Purposes, Temporal
P3	List (NAble)
P4	List, Purposes
P5	List (Able)
D1	List, Purposes
D2	List (NAble)
D3	Purposes
D4	List, Purposes, Permission
D5	Purposes, Features

Table 2. The table shows the components that allow us to meet the requirements in section III

V. AN ALGORITHM FOR THE MANAGEMENT OF AC

In order to show the ability of our model to define precisely the customized policies in accordance with the patient's need for privacy, we present an algorithm for the management of AC that uses the model. Like the model itself, the algorithm is modular, being composed, in fact, of different functions that use the different components of the model. In the algorithm it is possible to swap the order of one control function with another, obtaining a functioning that better suits certain needs. The algorithm allows or denies access to an object on the basis of the inputs that it receives.

The possible inputs are in below table:

Object identifier	the identifier of the clinical document in the EHR system, to which access is required
User identifier	the identifier of the subject who requires to operate on the object
Role	the role associated with the user in the EHR system;
Operation	the action required on the object;
Access purpose	the purpose, for which an object is accessed.

The output of the algorithm is PERMIT only if all the checks on access are satisfied. In fact, the algorithm consists of the checks in cascade made by the different functions presented below. The algorithm in "emergency mode" avoids several controls to speed access to the required object (as described in Requirement D5 in section III); for example, it does not make the presence control of the user in the list of authorized users or the control of access conditions. (Figure 2).

Before describing the control functions, we will show the algorithm.

Input: Object id, user id, role, operation, access purpose.
Output: decision {Permit, Deny}

```
switch (document.levelsecurity)
Case topsecret:
        If(checkAccess(user, object))
        then return PERMIT;
        else return DENY;
        end if
break;
Case secret:
        If(checkAccess(user, object))
        then return PERMIT;
        else return DENY;
        end if
break;
Case normal :
        if AccessPurposes= "Emergency"
        then if checkinEmergency(object,role)
        then return PERMIT;
        else return DENY;
        end if
        end if
 if checkNAble(user,role,object,operation)
 then return DENY;
        end if
        if not(checkPurpose(AccessPurposes, object,
operation))
        then return DENY;
        end if
        if checkList(user, role, object, operation)
        then if checkCondition(operation, object,
<condition>)
                        then return PERMIT;
                else return DENY;
                end if
        else return DENY;
        end if
break;
```

A. *Description of the functions*

Below there is the description of the functions used in the algorithm and illustrated in Figure 2.

- *The checkAccess(user, object)function*
  It receives as input **User identifier** and **Object identifier**. The function returns *true* if the user who requests access to the object is compliant with the policies about the security level of the requested document (*secret* or *top secret*).

- *The checkPurpose(Access Purpose, object, operation) function*
  It receives as input **Access purpose**, **Object identifier** and **Operation**. The function checks if the specified *Access Purpose* is in compliance with the purposes associated to the document (*Intended Purposes*) and the operation requested. If the check is successful, the function returns *true*.

- *The checklist(user, role, object, operation)function*
  It receives as input **User identifier**, **Role**, **Object identifier** and **Operation**.
  The function checks whether the user or the user role is included in the lists associated to the object for the specified operation. If so, the function returns *true*.

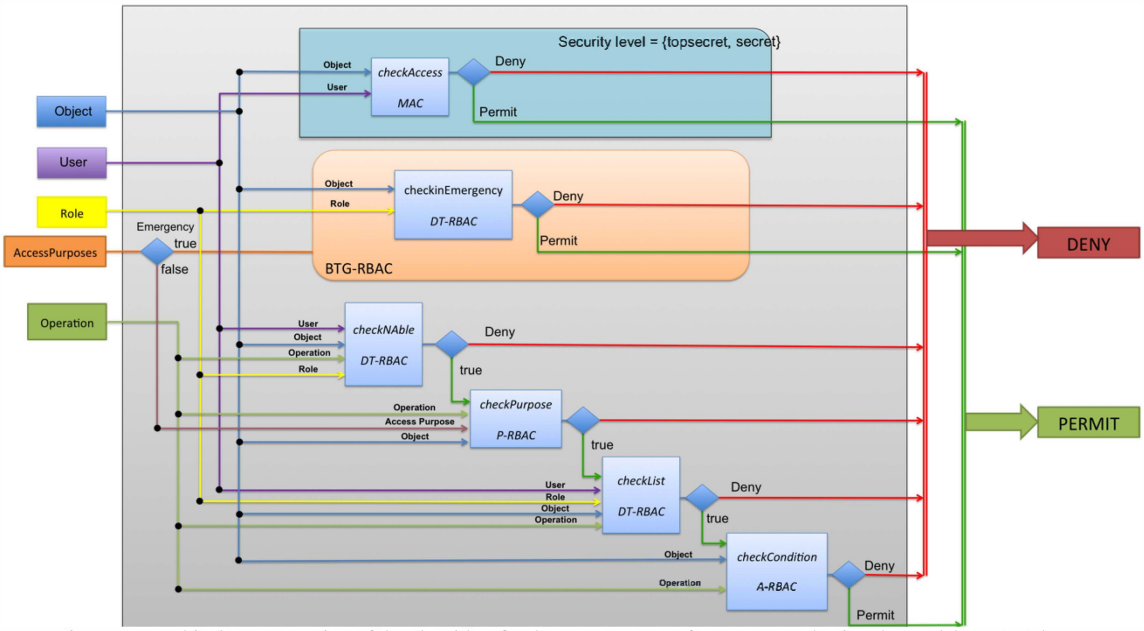

Figure 2. Graphical representation of the algorithm for the management of access control using the model presented

- *The checkinEmergency(object, role)function*
  It receives as input **Object identifier** and **Role**.
  The function first checks that the requested document is compatible with the emergency purpose (via **Purposes**); if so, it returns *true,* otherwise *false.* Next, it checks whether the specified role has the right to access in emergency mode (via **Features**). This function allows faster controls in the case of an emergency, providing a sort of Break the Glass AC model [14]. In fact, there is no cross checking of the object-list-operation, but the check occurs directly through **Features** and **Purposes**. Furthermore, the constraint conditions are relaxed (these are expressed by **Condition**). Obviously, the operations in emergency mode are associated with **Obligations**, such as storage in logger, the access information to the document or other obligations.

- *The checkNAble(user, role, object, operation) function*
  It receives as input **User identifier**, **Role**, **Object identifier** and **Operation**.
  The function checks if the role/user is present in the NAble lists associated to the operation on the given document. If she/he/it is in these lists, the system returns deny.

- *The checkCondition(operation, object)function*
  It receives as input **Object identifier** and **Operation**.
  The function retrieves the list of access conditions associated with the specific operation request. Next, it checks the compatibility of access in accordance with the conditions expressed in the **Conditions** component. For example it is possible to specify additional access restrictions, related to temporal or geographical conditions.

The proposed model is extremely dynamic and simple for the handling of customized access policies. The patient can easily indicate who has access to a certain health document contained in the EHR system, when and for which purpose.
The presented algorithm is modular, and in this way, it is possible to use only a subset of the function controls, or even invert the order of the functions. For example it is possible to swap the functions `checkinEmergency` and `checkNAble` to allow the patient to indicate subjects who

are not permitted to access a certain document, even in emergency mode.

VI. A CASE STUDY

Next, we describe a scenario to highlight a possible use of the introduced model and the algorithm associated with it.
We refer to a scenario in which a patient manages in a precise manner the confidentiality of the documents in her/his EHR using the components of the model and its support functionalities. In our scenario, first, a certain clinical document is inserted in the EHR by the healthcare organization, after which the patient modifies the privacy characteristics associated to the document to make it accessible to certain subjects in the system. Below, we distinguish the operations carried out by the healthcare organization (during the insertion of document in the EHR system) and the actions carried out by the patient for the modification of the rights of access to her/his clinical documents in the system.

Healthcare Organization

In our scenario John is the patient. He makes a dental panoramic radiograph at a healthcare organization. The healthcare organization inserts John's dental panoramic radiograph (DPR) into the EHR system. When the healthcare organization inserts the document, in order to define the access policies in accordance with the consent expressed by John, it has to specify the following attributes:

- **Security Level**: this expresses the level of security associated to the document (top secret, secret, normal). The healthcare organization indicates the security level chosen by John;
- **List of roles**: if the security level is normal, the healthcare organization indicates the roles of the operators that can have access to the document (for example general practitioners, nurses, etc.);
- **List of purposes**: this is the list of the purposes, for which the access to the document is allowed. The healthcare organization inserts the list of the purposes indicated by the patient for that document.

Considering the model in figure 1, when the healthcare organization inserts a document in the EHR system, it uses the following components: **List**, **Purposes**, **Object**, **Operations**, etc. Let us suppose that the configuration privacy is the following: the **security level** is normal; the **list of roles** is : Orthopedic Specialists, and General Practitioners (GP), the **list of purposes** is: medical care, and emergency.

Patient

Later, John wants to make his DPR accessible to his dentist Luke for clinical diagnosis purposes. Since Luke is not an orthopedic specialist, he has no right of access to John's DPR. John needs to create a list of users/roles (figure 3), in which Luke is enabled to access the DPR for **medical care** purposes (see figure 4). John can also specify the period of validity of the list associated with the document and other conditions.

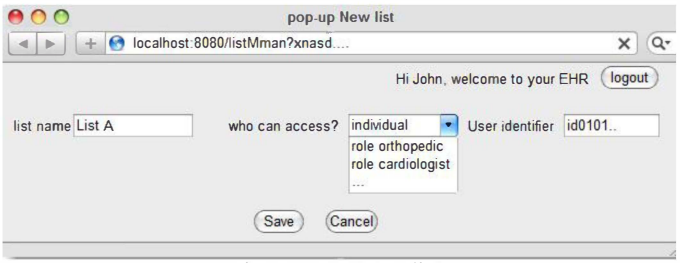

Figure 3. create new list

In figure 3 there is a screenshot of the support functionalities of the model "create new list". After John has created the list and associated it with the document, Luke is allowed to access the DPR to read it for the time specified by John. Let us now imagine a situation in which John wants to hide his DPR from a certain specialist orthopedic doctor named George. John therefore creates a list of non-authorized access (through *NAble* in figure 1) to the document, in which he inserts George (in figure 3 there is a screen shot of the support functionalities of the model "create new list").

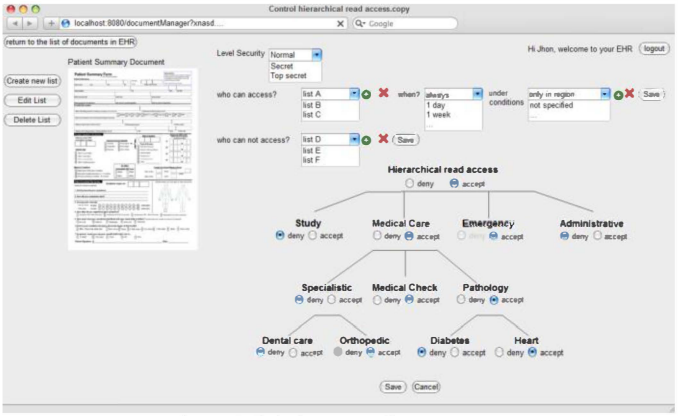

Figure 4. link document-lists-purposes

Now we show how the system reacts to attempts to access it by Luke and George (using the algorithm previously presented). If the user Luke accesses the system with the role of **dentist** and he wants to gain read access to John 's DPR with the purpose of **medical care**, the system will perform the following checks:

1. It checks the presence of the user Luke in the lists "*NAble*" associated with that document (in this example Luke is not present in the lists "*NAble*" of the DPR). The check produces *true*.
2. It checks the access purpose . The system compares the Access Purposes with the Intended Purpose associated with the document. The read operation is allowed, so the control is successful. The check produces *true*.
3. It checks the authorized lists associated with the document. In our case the user Luke is in the list of users who can access the document (in fact the list was created by John). The check produces *true*.
4. The system checks the conditions of access to the document, for example time constraints, location constraints, etc.

5. The system provides the grant, allowing Luke to read the DPR document.

If George accesses the system with the purpose of **medical care**, the DPR document will not be visible. In this case, the system excludes the user George from viewing the document, since he is present in the list of *NAble* access to the document. The check to the point 1 (described before) would give a *deny*.

VII. CONCLUSIONS

In this paper we have introduced a new access control model for an EHR system through adding further components to several different models, in order to obtain a multi-level and attribute-based solution with a dynamic management of the privacy policies. The added components respond, on the one hand, to the patients' need for privacy and, on the other, to their need for flexibility in the definition and management of the access policies.

We have identified the requirements for the realization of an access control model for EHR systems arising from i) the patient, who the documents refers to, ii) the healthcare organizations holding the data, and iii) the international, national and local directives and guidelines, such as HIPAA [13,15]. Our model aims at meeting these requirements.

We intend to extend the proposed model through the introduction of other components (for example the View-based component) in order to satisfy better the need for privacy in EHR systems. Considering the advent of the Cloud Computing paradigm and the concrete possibility of using this paradigm to realize an EHR system, it would be useful to develop our AC model in order to use it in the context of Cloud Computing, taking into account the security requirements of this paradigm.

Another interesting evolution of our model is linked to the introduction of a mechanism that allows the certification of the input information in the AC model. In fact, an EHR system is usually composed of a federation of different and heterogeneous systems, distributed over a wide geographical area, which must render it possible to grant the control of access in a federate manner and thus a secure and certified exchange of the “access information”. A possible further development is the introduction of our model into an implementation that uses a XACML architecture for the exchange of the information for the access control. In this way, it would be possible to obtain a prototypal solution for the identification of the federated authorization.

ACKNOWLEDGMENT

The work reported in this paper has been partially supported by the project ”Evoluzione e interoperabilita’ tecnologica del FascicoloSanitarioElettronico”, Agreement DDI-CNR, 18 June 2012, Prot. AMMCNT-CNR N. 53060, 31/08/12.References.

REFERENCES

[1] Iakovidis, I.: Towards Personal Health Record: Current Situation, Obstacles and Trends in Implementation of Electronic Healthcare Record in Europe. International Journal of Medical Informatics 52(1–3), 105–115 (1998)

[2] Lampson, B. W., "Dynamic Protection Structures," AFIPS Conference Proceedings, 35, 1969, pp. 27–38

[3] Bell, D. E., and L. J. LaPadula, Secure Computer Systems: Mathematical Foundations and Model, Bedford, MA: The Mitre Corporation, 1973. See also D. E. Bell and L. J. LaPadula, Secure Computer System: Unified Exposition and MULTICS Interpretation, MTR-2997 Rev. 1, Bedford, MA: The MITRE Corporation, March 1976, and ESD-TR-75-306, rev. 1, Electronic Systems Division, Air Force Systems Command, Hanscom Field, Bedford, MA 01731.

[4] http://csrc.nist.gov/publications/history/bell76.pdf. (Access date: 22 August 2013)

[5] Ferraiolo, D. F., J. Cugini, and D. R. Kuhn, "Role-Based Access Control (RBAC): Features and Motivations," in Proceedings of the 11th Annual Computer Security Application Conference, New Orleans, LA, December 11–15 1995, pp. 241–248.

[6] Elisa Bertino, Piero Andrea Bonatti, and Elena Ferrari. TRBAC: a temporal role-based access control model. In RBAC '00: Proceedings of the _fth ACM workshop on Role-based access control, pages 21.30, New York, NY, USA, 2000. ACM Press.

[7] Hai-bo Shen; Fan Hong, "An Attribute-Based Access Control Model for Web Services," Parallel and Distributed Computing, Applications and Technologies, 2006. PDCAT '06. Seventh International Conference on , vol., no., pp.74,79, Dec. 2006 doi: 10.1109/PDCAT.2006.28

[8] H. Oberholzer. A privacy protection model to support personal privacy in relational databases. Technical report, Rand afrikanns university, May 2001.

[9] Yoonjeong Kim; Eunjee Song, "Privacy-Aware Role Based Access Control Model: Revisited for Multi-Policy Conflict Detection," Information Science and Applications (ICISA), 2010 International Conference on , vol., no., pp.1,7, 21-23 April 2010 doi: 10.1109/ICISA.2010.5480349

[10] Naikuo Yang; Barringer, H.; Ning Zhang, "A Purpose-Based Access Control Model," Information Assurance and Security, 2007. IAS 2007. Third International Symposium on , vol., no., pp.143,148, 29-31 Aug. 2007 doi: 10.1109/IAS.2007.29

[11] http://csrc.nist.gov/rbac/sandhu-ferraiolo-kuhn-00.pdf. (Access date: 11 July 2013)

[12] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. (Access date: 13 September 2013)

[13] Carrion, I.; Aleman, J.L.F.; Toval, A., "Assessing the HIPAA standard in practice: PHR privacy policies," Engineering in Medicine and Biology Society,EMBC, 2011 Annual International Conference of the IEEE , vol., no., pp.2380,2383, Aug. 30 2011-Sept. 3 2011 doi: 10.1109/IEMBS.2011.6090664

[14] Ferreira, A.; Chadwick, D.; Farinha, P.; Correia, R.; GansenZao; Chilro, R.; Antunes, L., "How to Securely Break into RBAC: The BTG-RBAC Model," Computer Security Applications Conference, 2009. ACSAC '09. Annual , vol., no., pp.23,31, 7-11 Dec. 2009 doi: 10.1109/ACSAC.2009.12

[15] http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/ (Access date: 16 September 2013)

[16] M. Ciampi, G. De Pietro, C. Esposito, M. Sicuranza and P. Donzelli, "A federated interoperability architecture for health information systems" in press at the international journal of internet protocol technology, 2013