Application of Privacy-aware Role-based Access Control Model in IHE-XDS

Daniya Dauletbek[a], Shi-Zhong YUAN[b]

School of Computer Engineering and Science, Shanghai University, Shanghai, China
[a]daniya.dauletbek@gmail.com, [b]szyuan@shu.edu.cn

Abstract: Integrating the Healthcare Enterprise (IHE)'s Cross-Enterprise Document Sharing (XDS) profile is an open standards-based architecture specification for EHR systems. In EHR systems, it is necessary to provide a mechanism for access control to protect security and privacy of patient data. On the basis of related studies, this paper addresses the issue of access control and privacy protection of privacy data in XDS-based EHR systems, aiming to identify a suitable, privacy-aware role-based access control model based on specific access requirements for IHE-XDS. Privacy-aware role-based access control model is an extension model of RBAC model. It not just has the benefits of RBAC, but additionally adds restrictions on the permission assignment for the roles by using the purpose enforcement and privacy-aware access control enforcement. The proposed model could further protect privacy data, while decreasing the complexity of the role assignment.

1. Introduction

The XDS (Cross-enterprise Document Sharing) integration specification proposed by the IHE (Integrating Healthcare Enterprise) is used to solve the problem of cross-system information sharing. Medical information on IHE-XDS systems is sensitive and should be protected from unauthorized access. So for IHE-XDS systems it is important to guarantee the confidentiality and integrity of information and the privacy of patients. In order to meet these needs a generally utilized approach such as Role-Based Access Control (RBAC) model, which is a fundamental security obstruction for securing information in healthcare information system is used. The RBAC model is an alternative to the traditional access control models and it is an extensible and flexible access control model. The basic idea of RBAC is to introduce the concept of roles between users and access, connecting the users and roles to control the user's access to system resources by authorizing the role. Although the main consideration of the RBAC model is the protecting security of the system, but it is not intended to enhance the privacy policy because of the lack of three important elements of the privacy policy that described in the OECD (Organization for Economic Co-operation and Development) Guidelines, such as purpose binding, conditions and obligations. The types and possibilities of inconsistencies between policies also will increase, so the models applicable to describe the privacy protection such as Privacy-Aware RBAC (P-RBAC) by Q Ni et al. [9] and Purpose-Based Access Control model by JW Byun et al. [11] have been proposed. In these two models Purpose-Based Access Control model [11] is a comprehensive approach for privacy preserving access control based on the notion of purpose, which describes the reason(s) for data collection and processing and organized in a tree structure. The motivations for adopting purpose based approach are the fundamental policies for private information concern with which data object is used for what purposes. Purposes in this approach are divided into two categories: intended purpose and access purpose. Intended purposes tell how data should be used and access purpose tells how data will be used. One of the important improvements of the Privacy-Aware RBAC model [9] that has mentioned above is that it changes the description of permissions and introduces elements such as purpose, condition, and obligation. This model is extended model of the well-known RBAC model in order to provide full support for expressing highly complex privacy-related policies. Consistent with the classic RBAC model and according to the different model functions Privacy-Aware RBAC model contains a series of conceptual models such as Core P-RBAC, Hierarchical P-RBAC, Conditional P-RBAC and Universal P-RBAC. Compare to the traditional models, the two last mentioned models are more able to meet the requirements of IHE-XDS. In additional to meet the security and privacy requirement that mentioned in IHE profiles [21, 22] Basel Katt et al. [4] have already designed security architecture and proposed a Prototypical Implementation model. Although the model proposed by Basel Katt et al. can

satisfy the requirements of IHE-XDS, but due to lack of component of privacy-aware access control policies enforcement, cannot ensure the purpose and condition of access. Because this component is in charge of enforcing security and privacy access control policies on personal data, and these policies takes into account of preferences such as purposes for accessing data, entities the data may/may not be disclosed to, etc. Therefore, the model designed in this paper is the comprehensive model that based on the advantages of the two last models that mentioned above and it not only has the features of the role hierarchy of general RBAC, but also can provide the conditions, purposes and other fine-grained modules that required by privacy protection. So compared to the model proposed by Basel Katt et al. and the latest access control models, the model proposed in this paper can further enhance the security control and privacy protection of the privacy information of patient's. The model extends access control with the help of the notion of purpose, and takes the authorization management based on "purpose management". Through the purpose binding for the role and developing a common policy; In accordance with the different emphasis on patient's privacy, sets the purpose property for privacy data and formulates a personal policy. Under the premise of the unchanged general policy of the system, the patients can be adjusted personal policies with personal requirements of privacy. This paper elaborated on the idea of designing a Privacy-Aware RBAC model in IHE-XDS, presenting important elements of the model, such as conditions and purposes, and XACML policy execution.

2. Privacy-aware RBAC Model

The model designed in this paper is based on several features that belong to the RBAC and PRBAC model proposed by Yang et al.[13] and the P-RBAC model that proposed by Zhang et al.[7] This model is the model that comprehensively enforcing the security control and privacy protection by using the advantages of the components of Purposes, Conditions. The model includes the privacy protection logic and the access control policy of RBAC, in which the authorization assignment is needed in the privacy protection. Mainly combining the good aspects of the RBAC model and Purpose-Based RBAC model and create the comprehensive Privacy-Aware RBAC model that can be applied to IHE-XDS. Because the more complete and newer models are: Purpose-Based RBAC model and Privacy-Aware RBAC model. The model proposed in this paper is shown in the Figure1 below.

In the Figure1 User represents the user, indicates the subject. Role represents a kind of authority or title that has certain power and responsibility. Object represents the privacy information set that user requested. Action is an executable operation. Purpose indicates the purpose of the user accessing the privacy information that is collection of all purposes. Condition indicates the condition for the user to access the privacy information. In this model, the principle of role-based authorization, and assignment of permission, and the user obtains the permission to access the privacy information by being granted the appropriate role, and also the features of the condition is the same to the core P-RBAC model proposed by Q Ni et al. [9]. But the difference is that in this model further analyze in detail the Intended Purpose. The Intended Purpose consists of two parts, AIP (Allowed Intended Purpose), PIP (Prohibited Intended Purpose). Respectively indicates data can be accessed and prohibited for a particular access purpose. In this model, "Purpose" also possible to perform the responsibilities of access purpose. Because the privacy information can be only be accessed if the AC (Access Purpose) matches the IP (Intended Purpose). Because of this principle, Intended Purpose is associated to the component of "Purpose" in this model.

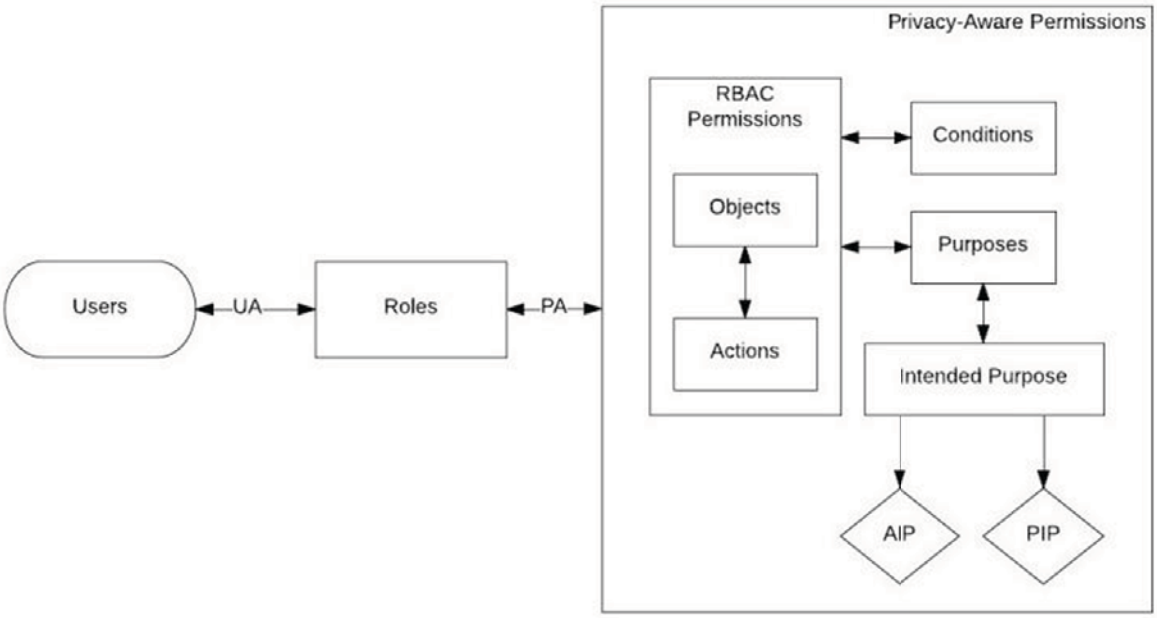

Figure 1. Privacy-Aware RBAC model in IHE-XDS

AP (Purpose) indicates Access Purpose, IP indicates the Intended Purpose, the allowed purpose of the Intended Purpose is AIP, prohibited purpose of the Intended Purpose is PIP. Thus, an Intended Purpose IP can be expressed as <AIP, PIP> . AIP and PIP are purpose sets. Where IP=<AIP, PIP> is an intended purpose, then IP^*=AIP↓-PIP↕,

IP_P=PIP↕. The meaning of IP^* is that, although the information provider gives the allowed intended purpose and prohibited intended purpose to indicate their willingness to use the information, but AIP and PIP will unavoidably occur conflict. Therefore, the principle of "prohibition of priority" is adopted here, that is, when occur conflicts between allowed purpose and prohibited purpose, determined as prohibited purpose. IP_P indicated a collection of information that cannot be accessed. If the PT is assumed to be the purpose tree, there is an intended purpose IP=<AIP, PIP> and an access purpose P on the PT, respectively. If $P \in IP^*$, then it is called P and IP matches, shows that under P, the information visitor can fully access the information.

Here:

- UA refers to (User Assignment): UA:⊆ User × Role
- PA refers to (Permission Assignment): PA⊆ Role × PP, refers to the many-to-many mapping between the role set and the permission set of access purpose.
- assigned_user: Role → 2User , represents that a role is mapped to a collection of user, indicates a user who granted a specific role. Its function is expressed as: assigned_user (r) = {u ∈ User | <u, r> ∈ UA}
- assigned_role: User → 2Role , represents that a user is mapped to a collection of role that represents the role that granted a specific user. Its function is expressed as: assigned_role (u) = {R ∈ Role | <u, r> ∈ UA}
- assigned_access_permission: Role → 2PP ,indicates that a role is mapped to a set of access that represents to grant access permission to the specific role. Its function is expressed as:
- assigned_access_permission (r) = {pp ∈ PP | <r, pp> ∈ PA}
- RBAC permissions: RBAC_Perm ⊆ O × A.
- P-RBAC permissions: P ⊆ O × A × C × Pu.

In the Privacy-Aware access control model, it is necessary to use a streamlined language form to express the conditional requirements in the privacy policy. That language uses a context variable (CV) to characterize, in the variables recorded privacy-related information that needs to be considered while executing the permissions. Although the conditional language LC_0 has only limited ability of expression, but for the privacy authority, LC_0 can characterize the conditional expression requirements in most of the permissions.

Conditional description language LC_0 Define CV as a set of context variables, for each variable x ∈ CV, there is a finite range of values defined as D_x, the range is represented by the relational operator equal sign (=) and the inequality (≠). In the various types of conditions, the definition of constant conditions for the use of logical operators false (F) and true (T) that expressed condition. The definition of the Meta conditions (ac, atomic condition) is the information expressed using the following expression: (x op_r v), where x∈ CV, v ∈ D_x, op_r ∈ {=, ≠} . The condition LC_0 is defined as:

- Constant condition is a component of LC_0 condition set.
- Meta-condition ac is LC_0 condition.
- If c_i, c_j are the two conditions in LC_0, then c_i, c_j and the relationship of $c_i \wedge c_j$ belongs to LC_0.

In order to show the ability of the model to be truly defined in the customization policy, according to the privacy needs of patient, proposed a graphic algorithm that uses in this access control model as shown in the Figure2.

3. Implementation Scheme of Privacy-Aware RBAC model for IHE-XDS

The research done by Basel Katt et al. [4] is a solution to solve the Access control and privacy issues in the system of distributed EHR system that utilizes IHE profiles. They put forward the security architecture and prototyping implementation in the context of the health @ net project. The Health @ net project is a core component of the development of an eHealth system according to IHE integration profile. They used the XACML as a policy language in the security architecture. The same language is used in the model designed in this paper. At the first let us approximately analyze the XACML before giving explanation to the model.

XACML policy execution consists of three main components:

- Policy
- Policy enforcement point (PEP)
- Policy decision point (PDP)

Figure 2. Graphic algorithm of authorization process of privacy enforcement

The XACML policy enforcement point (PEP) is the gateway that determines whether an operation is allowed or not. PEP accepts access requests, which are specially formatted XML documents that define a set of data values.

PEP forwards request to policy decision point (PDP).

The features of the components used in the Figure:

- Policy Administration Point (PAP) - This is the point at which the policy is managed.
- Policy Decision Point (PDP) - the point at which the authorization decision is evaluated and issued.
- Policy Enforcement Point (PEP) - A point that blocks user access requests for resources and enforces PDP decisions.
- Contextual Handler: Context information is associated with an access request, such as the purpose of accessing the data, the role of the requester, and so on.

Central Administration is the core of the security architecture that proposed by Basel Katt et al. [4], that is to say that all the privacy information exists in this part. In this architecture, the researchers have added PEP to the Registry, Consumer and Repository. In this research, in order to enhance the protection and security of privacy data, we would like to make some changes in the Central Administration of the model that proposed by Basel Katt et al. [4], and design a specific model. The main change made by this research is to connect the Central Administration directly to the PEP. And then establish a privacy-aware access control enhanced component between the information visitor and the information provider to enhance the security control and privacy protection of the privacy data. So, why do this research wants add PEP to the policy administration point and policy decision point? Because the benefits of PEP include:

- PEP is a single point of access.
- Policy is decoupled from applications/services.
- Policy can be managed independently of applications and services, so they can focus on providing business values.
- Auditing in PDP and PEP is simpler than auditing in many different applications/services.
- Implementation of change is simplified. Policies can be managed and deployed to explicit architectural functions (i.e. PAP and PDP).

Since unauthorized requests never get to the application / service (because it is blocked by PEP), it is not very easy to compromise the application. This is not the case if PEP and PDP are basically implemented in the applied security model. The PEP, PDP, PAP and PIP can be implemented using hardened, approved components.

Context awareness computing is becoming more and more important. Context-based authorizations will be simplified through isolated policy management and enforcement.

In general, the policy is essential to ensure that logical results are achieved. The purpose of policy management is to adapt the dynamic adaptability of the behavior of support in the process by changing the policy. This kind of system has two main management agents: 1) Policy decision point (PDP). 2) Policy enforcement point (PEP).

In the process of implementing Privacy-Aware RBAC model that can be applied for IHE-XDS, this paper has used some features of the XACML architecture. As shown in the Figure3.

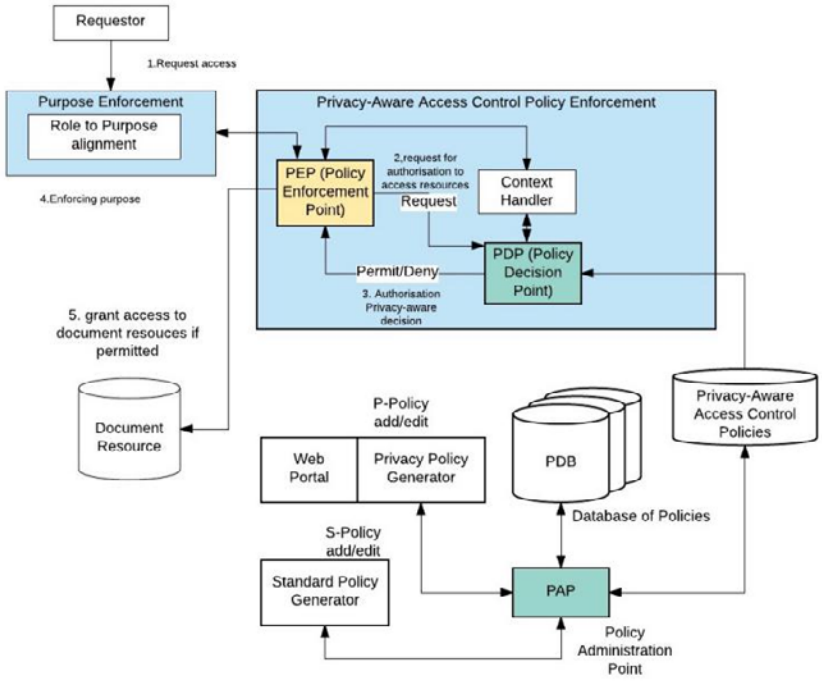

Figure 3. Implementation scheme of Privacy-Aware RBAC model for IHE-XDS

First of all, the PAP (Policy Administration Point) is connected to the PDB (Policy Library - DataBase of Policies), and the PAP (Policy Administration Point) enters the privacy access control policy to the Policy Library (PDB). After that the requestor sends an access request to the PEP (Policy Enforcement Point); the PEP will send the request to the Context Handler after the request is obtained. The Context Handler will translate the request into a standard format and send the request to the PDP, let it make the judgment of policy through DataBase of Policies. After the PDP obtains the judgment request, first, through the policy administration point will search the policy from the DataBase of Policies, and get the appropriate authorization policy, then, according to the privacy authorization policy, the PDP will send the result of decision to the Context Handler, after the Context Handler obtains the decision result, it will convert the result to the local format of the PEP (Policy Enforcement Point), and returns it to the PEP (Policy Enforcement Point). At last, PEP determines whether the authorization decision is made correct or incorrect, and if there is no error, it will it will execute the authorization decision and return the result to the requester through the execution part. The task of PAP is to manage the policies and policy sets, and make them available for PDP. These policies and policy sets refer to specific goals and complete policy. PEP is a component that receives a request when the access requestor wishes to take certain actions on the information (resource) and make a request. PEP will send the request to the Context Handler.

The Context Handler maps the request and attributes to the XACML request context and sends request to the PDP. When evaluating a request, the PDP requires some attributes and sends the attribute to the context handler through the query. At the same time, Purpose Enforcement part will be connected to the PEP (Policy Enforcement Point) and will strengthen the purpose of access through the PEP, requester can access to the Document Resource only if the role and the purpose are relatively accurate. A simple example of an access control policy using all of the above concepts is shown below. Using XML-based symbols to represent it, it is for illustrative purposes only.

```
Access Purpose
<policy>
  <name>policy-ID1</name>
  <target>ALL-ATTRIBUTES</target>
  <trigger>
    <expression>
      <and>
<condition>Request.Obj.Location=="PII.DB"</conditi
on>
        <condition>Context.Request.Purpose contained
in Context.PrivacyPreferences.Purpose</condition>
      </and>
    </expression>
  </trigger>
  <rules>
    <rule>
      <expression>
        <or>
<condition>Request.Role=="Admin"</condition>
          <and>
<condition>Request.Purpose=="surgicaldepartment"</c
ondition>
  <condition>Request.Role=="surgeon"</condition>
          </and>
          <and>
  <condition>Request.Purpose=="Research"</conditi
on>
<condition>Request.Role=="programmer"</condition>
          </and>
        </or>
      </expression>
      <action>
<decision>yes</decision>/action&gt;</action>
    </rule>
  </rules>
</policy>
```

In addition, proposed a graphic algorithm of PDP evaluating request as shown in Figure4.

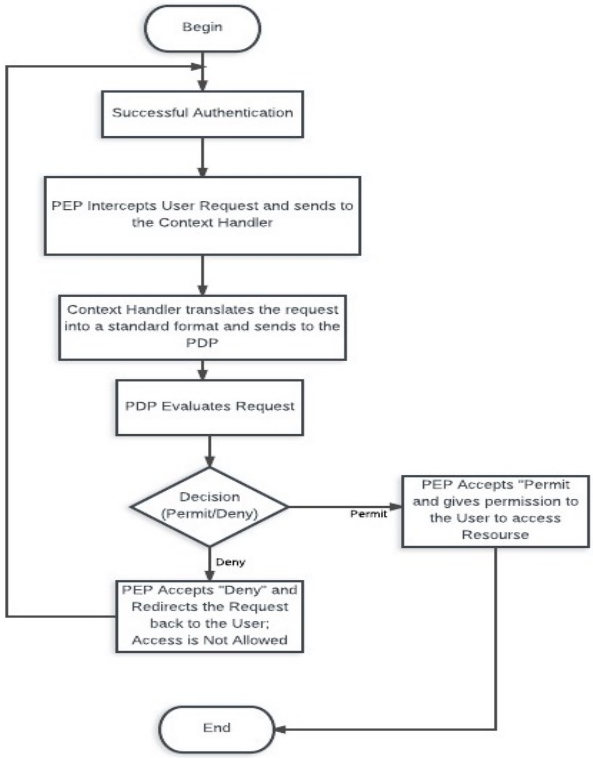

Figure 4. Graphic algorithm of PDP evaluating request

4. Discussion and Conclusion

This paper has discussed Privacy-Aware RBAC policies with conditions and purposes and also has presented the comprehensive model based on the advantages of RBAC model, notion of purpose and privacy-awareness that aims at enhancing the privacy policies in IHE-XDS. The work in this paper has extended previous work that has been proposed by scholars significantly in several aspects. First , it utilizes role describing the function and privacy requirement, and after that permission

assignments obtain the privacy authorization through playing roles and interact with other components such as purposes and conditions through receiving and sending data specified by roles. Second, it introduces privacy-aware access control policy enforcement, sets the enforcement point in the privacy policy, enforcement point just can obtain the privacy data if decision point has permitted the request, in this way the security of privacy data is enforced. But this paper is far from complete. Many details are bypassed, such as does not consider the time property of privacy data, detailed obligation mechanism and further validation, etc. Our future work is enriching and completing this model, to extend our model to deal with other elements of privacy such as obligations and complex conditions. Despite the fact that these elements are not easy to deal with, but they are essential parts of privacy protection.

References

1. Ferraiolo D., Kuhn R.. Role Based Access control [A]. In 15th NIST-NCSC National Computer Security Conference [C]. 1992:554-563
2. Health Information Technology for Economic and Clinical Health Act: Public Law 111-5.
3. IHE IT Infrastructure Technical Framework, Supplement 2012: Basic Patient Privacy Consents Integration Profile, IHE ITI Technical Committee, Revision 9.0 – Final Text, August 31, 2012.
4. Basel Katt, Ruth Breu, Michael Hafner, Thomas Schabetsberger, Richard Mair, Florian Wozak. Privacy and Access Control for IHE-Based Systems. Springer Berlin Heidelberg. 2009: pp 145-153
5. Lisa M. Kern, Rainu Kaushal. Health information technology and health information exchange in New York State: New initiatives in implementation and evaluation[J]. In: Journal of Biomedical Informatics 40(2007) S17-S20.
6. K.Irwin, T. Yu, abd W.H.Winsborough. On the modeling and analysis of obligations. In CSS'06, NewYork, NY, USA, 2006:134-143.
7. Zhang Y Q, Sun B, Liu J, et al. Study on fine-grained RBAC model based on AOP[J]. Electronic Design Engineering, 2011.
8. R.S.Sandhu, R.J.Coyne, H.L.Fwinstein, C.E.Youman. Role-Based Access Control Model. IEEE Computer Volume 29(2) ,Feb 1996: 38-47,.
9. Q Ni, D Lin, E Bertino, J Lobo. Conditional Privacy-Aware Role Based Access Control. Springer Berlin Heidelberg, 2007, 4734(4):72-89
10. Agrawal R, Kiernan J, Srikant R, Xu Y, Hippocratic databases.VLDB, HongKong, 200227.
11. JW Byun, N Li. Purpose based access control for privacy protection in relational database systems[J]. Vldb Journal International on Very Large Data Bases, 2008, 17(4):603-619
12. YANG N, BARRINGER H, ZHANG N. A purpose-based access control model[A]. Proc of the 3rd International Symposium on Information Assurance and Security (IAS)[C]. IEEE, 2007. 143-148.
13. Yang C Y, Liu C T, Tseng T W. Design and Implementation of a Privacy Aware Framework for Sharing Electronic Health Records[C]// International Conference on Healthcare Informatics. 2015:504-508.
14. Elisa Bertino, Carolyn Brodie, Seraphin Calo. Analysis of Privacy and Security Polices [J].IBM Journal of Research and Development, 2009:1-31.
15. Colombo Pietro, Ferrari Elena. Enforcement of Purpose Based Access Control within Relational Database Management Systems[A]. IEEE Transactions on Knowledge and Data Engineering, March 2014
16. Lampson B W. Protection of Information System. Proc 5thPrinceton Conference on Information Sciences and Systems, Princeton. 1971:437-44
17. Kabir M E, Wang H. Conditional purpose based access control model for privacy protection[C]// Twentieth Australasian Conference on Australasian Database. Australian Computer Society, Inc. 2009:135-142.
18. Organization for Economic Co-operation and Development. OECD guidelines on the protection of privacy and transborder flows of personal data of 1980. Available at http://www.oecd.org
19. Yoonjeong Kim et al. Privacy-aware Role Based Access Control Model: Revisited for Multi-Policy Conflict Detection [C]. Acm Research in Applied Computation Symposium, 2012:344-34720.
20. Ravi Sandhu, David Ferraiolo and Richard Kuhn. The NIST model for role-basedaccess control: towards a unified standard. Proceedings of the fifth ACM workshop on Role-based access control. Berlin, Germany, July 26-28 2000:47-63.
21. IHE Integrating the Healthcare Enterprise. IHE IT infrastructure white paper-hie security and privacy rhrough IHE. Technical report, 2007.
22. IHE Integrating the Healthcare Enterprise. IT infrastructure technical framework-basic patient privacy consents (BPPC). Technical report, 2007.