AN APPROACH TO ENFORCE CONTEXT-AWARE ACCESS CONTROL TO PROCESS-BASED HEALTHCARE SYSTEMS BUILD ON A GRID INFRASTRUCTURE

Vassiliki Koufi, Flora Malamateniou and George Vassilacopoulos
Department of Digital Systems, University of Piraeus, 80, Karaoli & Dimitriou Str., Piraeus 18534, Greece

Keywords: Grid portal application, Process, Role-based access control (RBAC), xoRBAC, Context.

Abstract: Healthcare is an increasingly collaborative enterprise involving a broad range of healthcare services provided by a number of geographically distributed and organizationally disparate healthcare providers. Grid technology has emerged as an integration infrastructure for shared and coordinated use of diverse data resources residing in the healthcare settings of a health district. Moreover, healthcare processes can be formed as compositions of web services that use grid database services to provide integrated healthcare information thus improving healthcare quality. Further improvement can be achieved by means of Grid portal applications developed on a wireless and mobile infrastructure as they provide to ubiquitous and pervasive access to healthcare processes at the point of care. In such environments, the ability to provide an effective access control mechanism that meets the requirement of the least privilege principle is essential. Adherence to the least privilege principle requires continuous adjustments of user permissions in order to adapt to the current situation. This paper presents an access control architecture for HDGPortal, a Grid portal application which provides access to workflow-based healthcare processes using wireless Personal Digital Assistants. The proposed architecture utilizes the xoRBAC component, which provides a role-based access control service that enables the enforcement of fine-grained context-dependent access control policies via context constraints. In particular, xoRBAC is integrated in our process-oriented healthcare environment which is build on top of a Grid infrastructure and is accessible through HDGPortal. Thus, the risk of compromising information integrity during task executions is reduced.

1 INTRODUCTION

Healthcare delivery is a highly complex process involving many individuals and organizations (Koufi and Vassilacopoulos, 2008). Providing readily access to integrated healthcare information at the point of care remotely requires a system architecture that enables collaboration and coordination among healthcare services and facilitates the mobility of healthcare professionals. To this end, a prototype Grid portal application, namely HDGPortal, has been developed that provides pervasive access to process-based healthcare systems (Koufi and Vassilacopoulos, 2008).

HDGPortal is a portal application that is used to run healthcare processes implemented in the Business Process Execution Language (BPEL). These processes invoke web services, while on execution, in order to provide integrated access to healthcare information scattered around disparate and geographically dispersed systems. These services are sophisticated high-level services that use Grid database services as basic primitives for their creation. Grid database services offer capabilities such as data federation and distributed query processing and are generated by using Open Grid Services Architecture - Data Access and Integration (OGSA-DAI) (Open Grid Services Architecture - Data Access and Integration (OGSA-DAI), 2008), a middleware product which is part of the Globus Toolkit (The Globus Toolkit, 2008). In the remainder of this paper, we refer to web services that are defined, deployed and executed using these service-oriented Grid computing infrastructures as Grid services (Emmerich, Butchart, Chen, Wassermann and Price, 2006).

As tight matching of permissions to actual usage and need is essential in healthcare applications, one important security requirement in HDGPortal is adherence to the least privilege principle. Its

Koufi V., Malamateniou F. and Vassilacopoulos G. (2009).
AN APPROACH TO ENFORCE CONTEXT-AWARE ACCESS CONTROL TO PROCESS-BASED HEALTHCARE SYSTEMS BUILD ON A GRID INFRASTRUCTURE.
In *Proceedings of the International Conference on Health Informatics*, pages 22-29
DOI: 10.5220/0001539900220029

enforcement requires continuous adjustments of user permissions to ensure that users assume the minimum sets of permissions required for the execution of each task of a healthcare process selected. To this end, changes in contextual information should be sensed during task executions and relevant actions should be fired in response to these changes.

xoRBAC is an open source software component that provides a policy decision point with an integrated policy repository for Role-Based Access Control (RBAC) policies (xoRBAC, 2008). In particular, xoRBAC provides an RBAC service that conforms to level 4a of the NIST model for RBAC (Neumann and Strembeck, 2001). In its current form, it preserves the advantages of role-based access control, and allows for the definition of "traditional" RBAC policies. Additionally it adds further flexibility through the specification of fine-grained context-dependent access control policies via context constraints (Neumann and Strembeck, 2003). On these grounds, the incorporation of xoRBAC in a process-based healthcare system build on top of a Grid infrastructure can offer significant benefits in the design and implementation of a context-aware access control mechanism.

This paper is mainly concerned with situations, often occurred in healthcare delivery, where the information requested by an authorized user needs to be available when and where needed. Thus, a context-aware access control mechanism is proposed that utilizes xoRBAC component and, hence, it incorporates the advantages of broad, role-based permission assignment and administration across object types, as in RBAC, and yet provides the flexibility for adjusting role permissions on individual objects during a BPEL process enactment according to the current context. During the execution of a workflow instance, changes in context information are sensed to adapt user permissions to the minimum required for completing a job. Relevant access control policies are enforced at both the BPEL task level and the Grid database service level.

2 RELATED WORK

In the last few years, there has been a trend towards using BPEL for Grid service composition (Emmerich, Butchart, Chen, Wassermann and Price, 2006). Security aspects, such as authentication and access control, are not standardized through BPEL, but are left to the implementation of BPEL compliant process engine (Mendling, Strembeck, Stermsek and Neumann, 2004; Thomas, Paci, Bertino and Eugster, 2007; Bertino, Crampton and Paci, 2006). Several studies have been conducted regarding the enforcement of access control in BPEL (Mendling, Strembeck, Stermsek and Neumann, 2004; Thomas, Paci, Bertino and Eugster, 2007; Bertino, Crampton and Paci, 2006; Dou, Cheung, Chen and Cai, 2005; Paci, Bertino and Crampton, 2008; Fischer, Bleimann, Fuhrmann and Furnell, 2007). Most of these studies argue that BPEL can benefit from incorporating properly enhanced role-based access control (RBAC) mechanisms (National Institute of Standards and Technology (NIST) RBAC, 2008).

In turn, grid middleware, namely Open Grid Services Architecture - Data Access and Integration (OGSA-DAI) (Open Grid Services Architecture - Data Access and Integration (OGSA-DAI), 2008), that facilitates data federation and distributed query processing through the use of grid database services provides relatively simple and static mechanisms regarding authorization and access control (Adamski, Kulczewski, Kurowski, Nabrzyski and Hume, 2007). In particular, OGSA-DAI mechanisms are written in a modular way so as to enable incorporation of application-specific security models in relatively straightforward fashion (Power, Slaymaker, Politou and Simpson, 2005). Hence, several studies have been conducted regarding the enhancement of these access control mechanisms (Adamski, Kulczewski, Kurowski, Nabrzyski and Hume, 2007; Power, Slaymaker, Politou and Simpson, 2005). Most of these studies argue that moving from identity-based to role-based access control mechanisms can offer significant benefits in the provision of effective access control over Grid middleware services (National Institute of Standards and Technology (NIST) RBAC, 2008).

In this paper we propose a security architecture that implements access control in the context of a pervasive process-based healthcare system build on a Grid infrastructure. The proposed architecture utilizes the xoRBAC component on both the BPEL and the Grid Database service level in order to enforce fine-grained context-dependent access control policies.

3 MOTIVATING SCENARIO

To illustrate the main principles of the security architecture incorporated into the HDGPortal, a sample integration project is described which is

concerned with the automation of a cross-organizational healthcare process spanning a health district. Typically, a health district consists of one district general hospital (DGH) and a number of peripheral hospitals and health centers. As patient referrals are usually made among various healthcare providers within a district (e.g. for hospitalization, for outpatient consultation or for performing specialized medical procedures), there is a need to ensure authorized access to the tasks comprising the relevant healthcare processes and, then, to patient information required through the execution of these tasks.

Suppose that a healthcare process is concerned with a radiological request issued by physicians on a ward round, for their patients. The radiological department receives each request, schedules the radiological procedures requested and sends a message to the requesting physician notifying him/her on the date and time scheduled for its performance. On performing the radiological procedure requested, the radiologist accesses the relevant part of the patient record and issues a radiological report, incorporating both the radiological images and the associated assessment, which is send to the requesting physician.

Figure 1 shows a high-level view of the healthcare process using IBM Websphere Workflow build-time tool (IBM Corporation. IBM Websphere Workflow – Getting Started with Buildtime V. 3.6, 2005). In this business process the hospital organizational units involved are the clinical department and the radiology department of a hospital and the roles participating in the healthcare process are physician (PHYS) and radiologist (RDD). Table 1 shows an extract of workflow authorization requirements regarding task execution and related data access privileges assigned to these roles, respectively.

From an authorization perspective, the healthcare process of Figure 1 surfaces several requirements with regard to task execution and Grid database services' invocation. These requirements include the following:

- *Restricted task execution*
  In certain circumstances the candidates for a task instance execution should be dynamically determined and be either a sub-group of the authorized users or only one, specific authorized user. For example, a request for performing a radiological procedure on a patient (e.g. CT or MRI), issued by a physician, should be routed only to the sub-group of on-duty radiologists who hold the relevant sub-specialty and the radiological report, issued by the radiologist, should be routed only to the requesting physician.
- *Restricted grid database service invocation*
  Given that a role holder can execute a specific task, he/she should be allowed to exercise a dynamically determined set of permissions on certain data only which are accessible via the associated Grid database services. For example, during the execution of the "IssueRadRequest" task, the relevant Grid database services invoked should allow a physician to write and read patient record data and to issue (write, edit and send) radiological requests only for his/her patients while on duty and only within the hospital premises.

Table 1: Extract of authorization requirements for the healthcare process of Figure 1 (Task execution and data access permissions).

1.	PHYSs may issue requests for radiological procedures on patients while on duty and within the hospital premises (IssueRadRequest).
1.1	PHYSs may write radiological requests for their current patients.
1.2	PHYSs may edit radiological requests for their current patients before sent.
1.3	PHYSs may send radiological requests for their current patients.
1.4	PHYSs may cancel radiological requests for their current patients after sent.
1.5	PHYSs may read patient records of their current patients.
2.	RDDs holding a specific sub-specialty may perform only relevant radiological procedures on patients (RerformRadRequest)
3.	RDDs may issue patient-oriented radiological reports on request by physicians (IssueRadReport).
3.1	RDDs may read patient record data before sending their radiological reports.
3.2	RDDs may write patient-oriented radiological reports for their current patients.
3.3	RDDs may edit patient-oriented radiological reports for their current patients before sent.
3.4	RDDs may send patient-oriented radiological requests for their current patients
3.5	RDDs may cancel patient-oriented radiological reports after sent.
3.6	RDDs may read past patient radiological reports prepared by them.
4.	PHYSs may receive patient radiological reports issued by radiologists only if requested by them (ReceiveRadReport).
4.1.	PHYSs may read the requested radiological reports on their patients.
4.2.	PHYSs may read patient records of their patients.

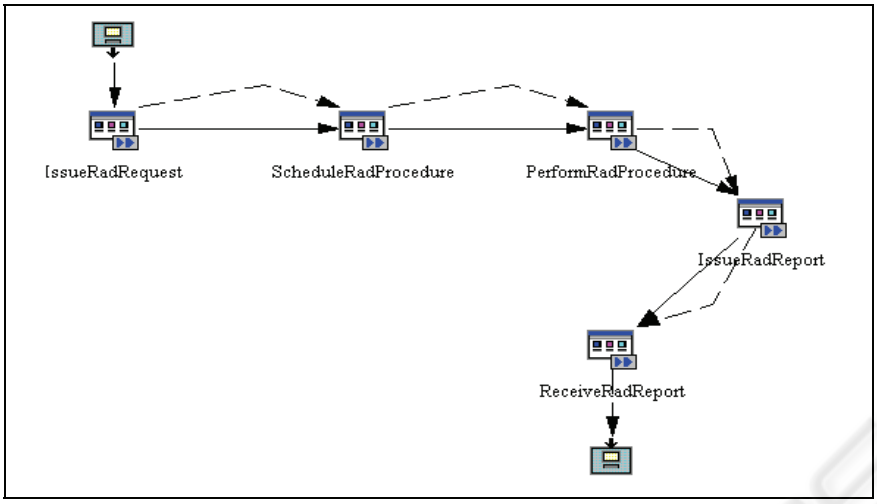

Figure 1: Radiological request process model using IBM WebSphere Workflow.

The above requirements suggest that certain permissions of the healthcare process participants depend on the process execution context. In particular, contextual information available at access time, such as proximity, location and time, can influence the authorization decision that allows a user to perform a task and, given this permission, to invoke the associated Grid database services. This enables a more flexible and precise access control policy specification that satisfies the least privilege principle.

4 SECURITY ARCHITECTURE

Figure 2 illustrates a high-level view of HDGPortal architecture, which is described by a three-tier model, comprising the PDA client, the server site of the DGH and the Grid which, in turn, comprises remote data resources. The latter are heterogeneous and reside in geographically distributed and organizationally disparate healthcare providers within a health district. HDGPortal's architecture requires enhanced security mechanisms with special focus on authorization and access control over the tasks comprising the BPEL processes and the underlying services (Grid database services and Grid services invoking them). Figure 3 illustrates a high-level view of the proposed security architecture which consists of a global access control service, residing on a server at the DGH site, and one local access control service, residing at each healthcare organization within the health district. Both services are making use of the xoRBAC access control component which provides an RBAC service that conforms to level 4a of the NIST model for RBAC (Neumann and Strembeck, 2001) and constitutes a core component of this architecture.

xoRBAC does not demand on a specific authentication mechanism, it only assumes that some authentication service is in place (Neumann and Strembeck, 2001). Therefore, in HDGPortal prototype authentication is performed by means of a sophisticated authentication environment based on X.509 certificates and SSL. In particular, Grid Security Infrastructure (GSI) authentication mechanism is used which defines single sign-on algorithms and protocols, cross-domain authentication protocols, and temporary credentials called proxy credentials stored in the MyProxy Server (MyProxy Credential Management Service, 2008). MyProxy is open source software for managing X.509 Public Key Infrastructure (PKI) security credentials (certificates and private keys) (MyProxy Credential Management Service, 2008). It combines an online credential repository with an online certificate authority to allow users to securely obtain proxy credentials when and where needed, without worrying about managing private key and certificate files (MyProxy Credential Management Service, 2008). In our environment, a MyProxy server is hosted on a server at the DGH site. Healthcare professionals use MyProxy to delegate credentials to the HDGPortal, which then is acting on their behalf. This is achieved by storing credentials in the MyProxy repository and retrieving them when logging in HDGPortal by typing in the MyProxy passphrase.

All web transactions are executed under the Secure Socket Layer (SSL) via HTTPS.

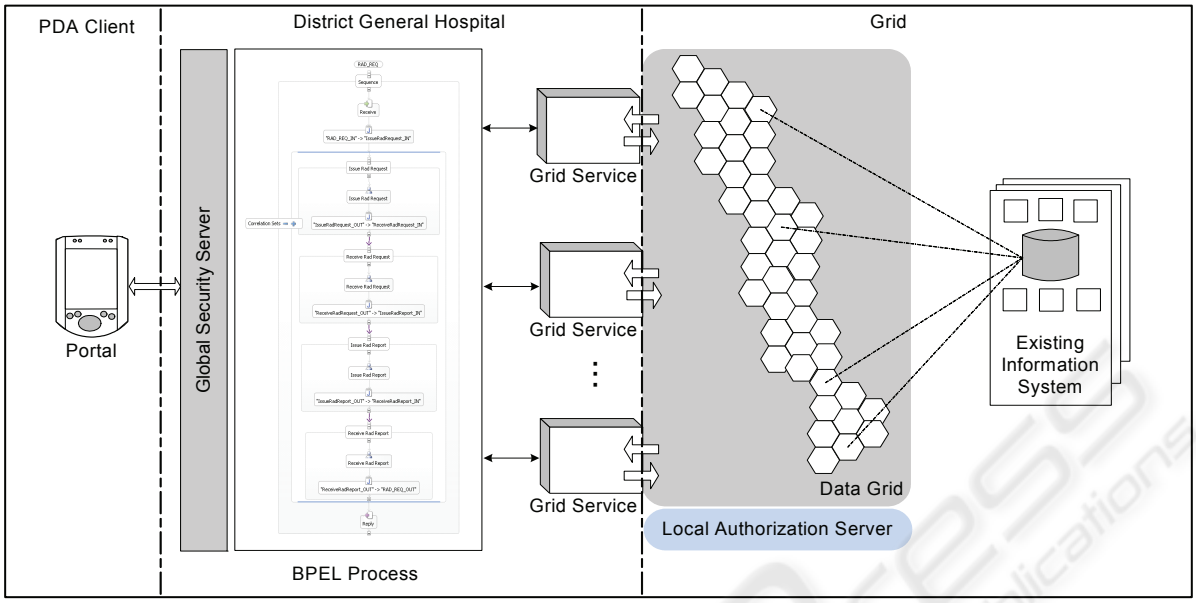

Figure 2: System Architecture.

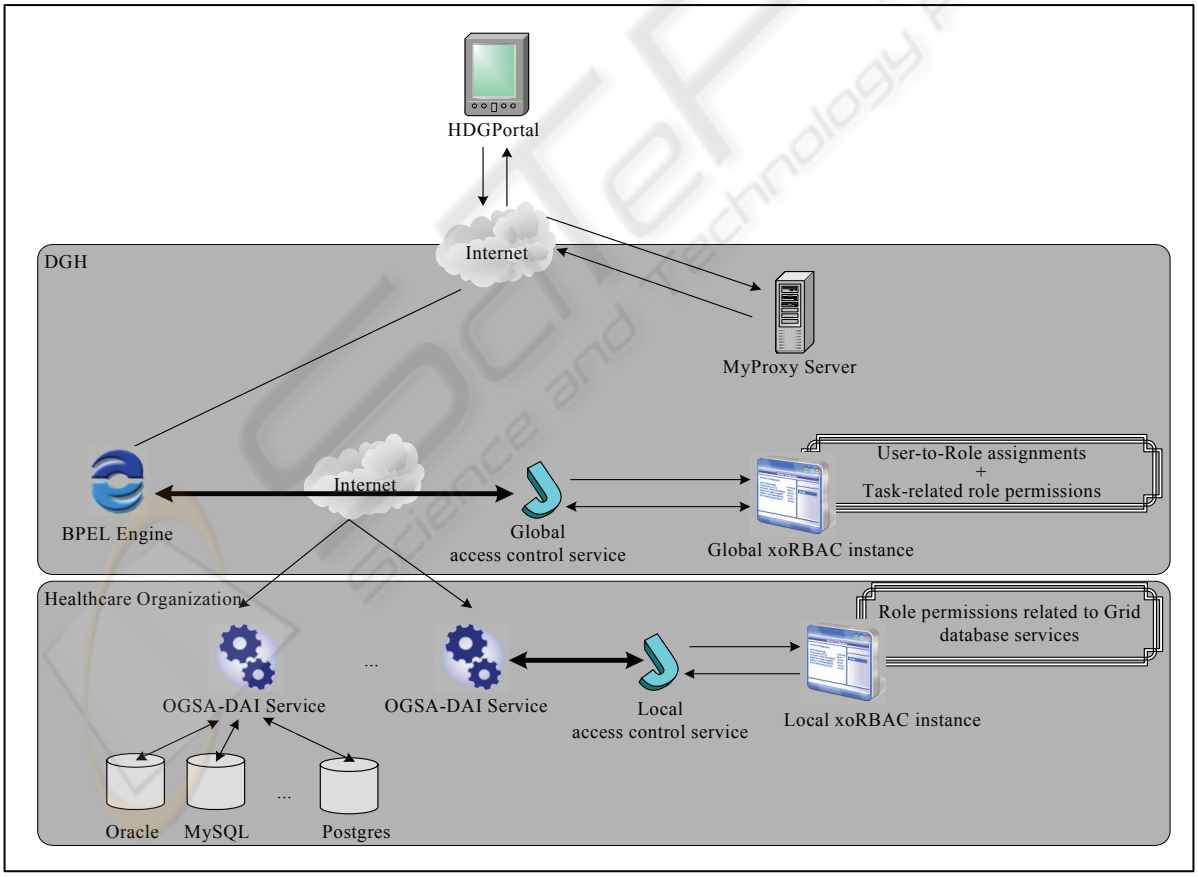

Figure 3: Security Architecture.

4.1 Access Control Mechanism

In HDGPortal prototype, access control is provided at two levels: the BPEL task level and the Grid database service level (Koufi and Vassilacopoulos, 2008). Hence, a middleware-based access control mechanism has been developed which is employed to mediate between subjects (healthcare professionals) and objects (BPEL tasks and Grid database services) and to decide whether access of a given subject to a given object should be permitted or denied by taking into account the current context. In particular, the Java Authentication and Authorization Service (JAAS) (Java Authentication and Authorization Service, 2008) was used for the development of:

- an, external to the BPEL engine, access control service (global access control service) that regulates user access to BPEL tasks comprising the healthcare processes. These tasks are hosted on the BPEL engine at the DGH site.
- an, external to OGSA-DAI, access control service (local access control) that enhances its mechanism by adding context-awareness features. In particular, this service regulates access to Grid database services which form the basic primitives for the generation of the Grid services invoked by the relevant tasks. Grid database services are hosted on web servers at healthcare organizations' sites.

The above access control services utilize two kinds of xoRBAC instances. In particular,

- the global access control service uses a xoRBAC instance (global xoRBAC instance) for the definition of permissions on the corresponding BPEL tasks comprising the healthcare processes. These permissions are assigned to roles which are, in turn, assigned to healthcare professionals. The global xoRBAC instance resides on a server at the DGH site.
- each local access control service uses a xoRBAC instance (local xoRBAC instance) for the definition of permissions on the corresponding Grid database services invoked by the relevant BPEL tasks. The local xoRBAC instance resides on a server at each healthcare setting.

According to the proposed mechanism, each request for a task execution, issued by a healthcare professional, is captured and passed to the global xoRBAC instance which decides whether access should be granted. As each task execution invokes exactly one Grid service, allowing task execution means allowing the invocation of the underlying Grid service. The decision for granting access or not is taken in accordance to the active role set of a subject (healthcare professional) and the context holding at the time of the attempted access. During task execution, the relevant Grid service is invoked which, in turn, may involve the invocation of a number of Grid database services residing at different sites within a health district. Each request for the invocation of a Grid database service is captured at the site hosting the service and passed to the corresponding local xoRBAC instance which decides whether access should be granted with regard to the current context.

4.2 Context Information Management

In the HDGPortal prototype, the contextual information is determined by a pre-defined set of attributes related to:

- the user (e.g. user certificate, user/patient relationship),
- the environment (e.g. client location and time of attempted access) and
- the data resource provider, namely to the healthcare organization (e.g. local security policy).

For example, the permissions of a physician using HDGPortal on his/her PDA, are adapted depending on his/her identity (included in the proxy certificate), location and time of access as well as the security policy of each healthcare organization where a portion of the requested information is stored.

Context information relevant to access control is used for the definition of context constraints which enable the enforcement of fine-grained context-dependent access control policies. In xoRBAC component, enforcement of such policies is achieved via the *dynamic constraint manager* sub-system. The latter comprises the *environment mapping* which captures context information via physical and logical sensors, and the *constraint evaluation* which uses the collected values to evaluate the relevant context constraints associated with a certain conditional permission (Guth, Neumann and Strembeck, 2003). Context constraints are composed of context conditions through which they combine and interrelate the measurements of the sensors (Guth, Neumann and Strembeck, 2003).

In HDGPortal, context information is captured by a set of xoRBAC's logical sensors. These consist only of software components and are used to gather information extracted from system internal sources (e.g. the IP address of a certain device, information stored in databases or log files, the status of other applications or services, CPU ID, CPU state, network load and so on) (Neumann and Strembeck, 2003). Currently, xoRBAC implements three types of logical sensors, namely Localhost, Database and Flatfile Sensors, respectively. HDGPortal utilizes these types of sensors in conjuction with an Authentication Sensor. The Database and Flatfile Sensors are used in their current form while Localhost Sensor has been extended in order to provide additional information (i.e. the client's IP). Moreover, the Authentication Sensor is a logical sensor build from scratch which is concerned with user-related context information (i.e. the validation of the user's proxy certificate). In particular, HDGPortal uses:

- *Localhost Sensor* for capturing context information related to the environment (i.e. time of attempted access and client location). Time is captured via clock, a context function which is already exported by LocalhostSensor. In order for client location to be captured, LocalhostSensor is extended with an additional context function, namely clientLocation which processes the HTTP headers of each client request in order to extract the client's IP and determine whether the healthcare professional using it is in hospital premises at the time of the attempted access.
- *Database Sensor* for capturing part of the context information related to the user (i.e. user/patient relationship). This information is retrieved by querying the relevant MySQL database. One important disadvantage of this sensor though is that in-depth knowledge of the underlying database schema is required.
- *Flatfile Sensor* for capturing context information relevant to the data resource provider, namely the healthcare setting hosting part of the patient's medical record. This information is the provider's local access control policy regarding certain individuals (i.e. an access control list) and is stored in a file at the provider's site. In particular, if there is an entry for a user requesting access to a data resource then the authorization decision is based on the rights assigned to him via that entry and overrides the decision deducted by taking into account the rest of the information comprising the context information model.
- *Authentication Sensor* for checking the validity of the credentials used by each user requesting access to the system.

In the case of the healthcare process described in Section 3, a physician may execute the task "IssueRadRequest" (i.e. issue a request for a radiological procedure on one of his/her patients) while on duty and within the hospital premises. Thus, the context attributes to be taken under consideration in the relevant authorization decision are:

1. current_date_&_time
2. duty_date_&_time_interval
3. client_IP_address
4. in_premises_IP_address

The values of these attributes are collected via a subset of the above mentioned sensors. The context conditions that must evaluate to true in order for access to be granted to the physician are:

1. current_date_&_time in duty_date_&_time_ interval
2. client_IP_address is-a in_premises_IP_ address

These context conditions compose the context constraint which is associated with the conditional permission on the task "IssueRadRequest". This constraint is evaluated by the *constraint evaluation* component of the xoRBAC's *dynamic constraint management* sub-system whenever access to the task is requested.

5 CONCLUDING REMARKS AND FUTURE WORK

Development of pervasive applications that provide readily access to integrated healthcare information at the point of care, introduces security risks especially with regard to authorization and access control. Hence, relevant mechanisms must be in place that can conveniently regulate user access to information while providing confidence that security policies are faithfully and consistently enforced within and across organizations residing in a health district. In particular, when adherence to the least privilege principle is considered a prominent feature of a system, the incorporated access control mechanism should provide tight, just-in-time permissions so that authorized users get access to specific objects

subject to the current context. The access control mechanism presented in this paper meets the aforementioned requirements and is embedded into a Grid portal application, namely HDGPortal. In particular, the mechanism ensures authorized execution of BPEL tasks and invocation of relevant Grid database services in accordance with the current context. To this end, a number of xoRBAC instances are integrated at both the BPEL and the Grid database service level as policy decision points. Thus, a tight matching of permissions to actual usage and need is ensured through the specification of fine-grained context-dependent access control policies.

Currently, the pieces of information influencing authorization decisions in xoRBAC are rather limited. This fact, suggests directions for future work. In particular, the enrichment of the context information model used by xoRBAC may enable the enforcement of even more effective access control policies in healthcare. Furthermore, certain disadvantages that appear in the mechanisms that are currently used for the collection of the context information may constitute an interesting topic for further research.

REFERENCES

Koufi, V., Vassilacopoulos, G., 2008. HDGPortal: A Grid Portal Application for Pervasive Access to Process-Based Healthcare Systems, In PervasiveHealth'08, 2nd International Conference in Pervasive Computing Technologies in Healthcare.

Emmerich, W., Butchart, B., Chen, L., Wassermann, B., Price, S., 2006. Grid Service Orchestration Using the Business Process Execution Language (BPEL), Journal of Grid Computing (2006) 3: 283-304.

Mendling, J, Strembeck, M, Stermsek, G, Neumann, G., 2004. An Approach to Extract RBAC Models for BPEL4WS Processes, Proceedings of the 13th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises.

Thomas, J., Paci, F., Bertino, E., Eugster, P., 2007. User Tasks and Access Control over Web Services, Proceedings of the 15th IEEE International Conference on Web Services, 2007.

Bertino, E., Crampton, J., Paci, F., 2006. Access Control and Authorization Constraints for WS-BPEL, Proceedings of the IEEE International Conference on Web Services, 2006.

Open Grid Services Architecture - Data Access and Integration (OGSA-DAI), http://www.ogsadai.org.uk/.

Adamski, M., Kulczewski, M., Kurowski, K., Nabrzyski, J., Hume, A., 2007. Security and Performance Enhancements to OGSA-DAI for Grid Data Virtualization, Concurrency and Computation.: Practice and Experience, 2007.

Dou, W., Cheung, SC., Chen, G., Cai, S., 2005. Certificate-Driven Grid Workflow Paradigm Based on Service Computing, Lecture Notes in Computer Science (2005) 3795: 155-160.

Power, D., Slaymaker, M., Politou, E., Simpson, A., 2005. A Secure Wrapper for OGSA-DAI, Lecture Notes in Computer Science (2005) 3470: 485-494.

IBM Corporation. IBM Websphere Workflow – Getting Started with Buildtime V. 3.6, 2005.

Java Authentication and Authorization Service, http://java.sun.com/javase/6/docs/technotes/guides/security/jaas/JAASRefGuide.html.

National Institute of Standards and Technology (NIST) RBAC, http://csrc.nist.gov/groups/SNS/rbac/

Neumann, G., Strembeck, M., 2001. Design and Implementation of a Flexible RBAC-Service in n Object-Oriented Scripting Language. Proceedings of CCS'01, November 5-8, 2001, Philadelphia, Pennsylvania, USA.

Neumann, G., Strembeck, M., 2003. An Approach to Engineer and Enforce Context Constraints in an RBAC Environment, Proceedings of SACMAT'03, June 2-3, 2003, Como, Italy.

The Globus Toolkit, http://www.globus.org/

xoRBAC, http://wi.wu-wien.ac.at/home/mark/xoRBAC/index.html

Neumann, G., Strembeck, M., 2003. An Approach to Engineer and Enforce Context Constraints in an RBAC Environment, ACM Transactions on Information and System Security, Vol. 7, No. 3, August 2004, pp 392-427.

MyProxy Credential Management Service, http://grid.ncsa.uiuc.edu/myproxy/

Paci, F., Bertino, E., Crampton, J., 2008. An Access-Control Framework for WS-BPEL, International Journal of Web Services Research, Vol. 5, Issue 3, pp. 20-43.

Fischer, K.P., Bleimann, U., Fuhrmann, W., Furnell, S.M., 2007, "Security policy enforcement in BPEL-defined collaborative business processes", Proceedings of the 1st International Workshop on Security Technologies for Next Generation Collaborative Business Applications (SECOBAP'07).

Guth, S., Neumann, G., Strembeck, M., 2003. "Experiences with the Enforcement of Access Rights Extracted from ODRL-based Digital Contracts". In DRM'03, 3rd ACM Workshop on Digital Rights Management.