An Access Control Framework for Pervasive Mobile Healthcare Systems Utilizing Cloud Services

Mikaela Poulymenopoulou, Flora Malamateniou, and George Vassilacopoulos

Department of Digital Systems, University of Piraeus, Piraeus 185 34, Greece
{mpouly,flora,gvass}@unipi.gr

Abstract. Mobile in conjunction with cloud computing can fulfil the vision of "Pervasive Healthcare" by enabling authorized healthcare participants to access services and required patient information without locational, time and other restraints. Of particular importance on such healthcare systems that incorporate mobile devices and cloud services is protecting the confidentiality of patient information. On these grounds, this paper proposes an access control framework for providing role-based context-aware authorization services with regard services invocations and patient information accesses. According to this, authorization decisions are taken according to contextual constraints that result from the domain ontology inferring that is used to represent context information.

Keywords: context-aware, access control, mobile and cloud computing, healthcare.

1 Introduction

Pervasive computing with the use of appropriate technologies like mobile technology, wireless networks and cloud computing has received considerable attention in the healthcare field recently for providing anytime and anywhere access to appropriate patient information and services to users during healthcare delivery process according to their changing environment [1], [2]. Healthcare delivery is inherently a decentralized process with participating users crossing many institutional boundaries. With the use of a pervasive healthcare system, participating users without locational and time restraints can access context-aware services existing on cloud by their mobile devices in order to view, update and share patient information that is usually structured in the form of XML documents and are also stored to the cloud [2], [3]. In such a pervasive healthcare system, it is important to meet the global security requirements of the healthcare organization(s) involved in the healthcare processes in order to protect the confidentiality of patient information, whilst at the same time allow authorized users to access it conveniently. This is a crucial requirement in the unpredictable environment of healthcare where context is often changing and users change roles at runtime. Thus, there is a need for an access control policy that is adaptable according to the active context, in a way that when the context changes the access control policy must reflect this change [4], [5], [6], [7].

K.S. Nikita et al. (Eds.): MobiHealth 2011, LNICST 83, pp. 380–385, 2012.

On these grounds, in this paper emphasis is on a security framework proposed to provide discretionary role-based and context-aware access control services with regard to services executions and patient XML documents (existing on the cloud) accesses according to an access control model developed. This work is motivated by our involvement in an emergency healthcare project that is still under development and concerns the implementation of a pervasive emergency healthcare system with the use of mobile and cloud computing. To illustrate the feasibility and applicability of the proposed security framework a simplified version of the emergency healthcare process is described.

2 Methods

In Figure 1 the proposed context-aware access control framework is presented. At cloud servers there exists an application server that hosts the web and cloud (provided by the cloud vendor) services and the context manager (CM) that acts as a mediator among users' environment and the semantic knowledge base. The CM uses an inferring engine for context reasoning. In addition, there exists the access control mechanism (ACM) that takes context-based authorization decisions for (cloud and web) services invocations and XML documents accesses existing on cloud. Moreover, at cloud servers there exists a database server where the access control policy and the knowledge base are stored. It is assumed that during healthcare delivery, authorized staff uses a mobile application on their mobile devices that sends context information from users environment to the CM. On users' request, the mobile application calls services existing on cloud that are orchestrated into workflows in order to create, view and update the XML documents with patient medical data.

Context information might be domain-dependent like the subjects (users) and objects (patients) involved in the healthcare processes as well as the relationships between them or might be domain-independent such as this related to the environment (e.g. time) [2], [5], [6]. In order to allow the ACM to interpret context accurately and to have a common understanding among the participating healthcare organizations, context information was organized in the form of a domain ontology using Ontology Web Language (OWL) which also enables context sharing in a semantic way and context reasoning. Those OWL files are stored to the knowledge base and additionally Semantic Web Rule Language (SWRL) rules were written in order to capture the relationships between subjects and objects [4], [5]. In particular, after services execution appropriate context information is sent to the CM that creates any individuals to the domain ontology. Then, the inferring engine infers the domain ontology and the relevant SWRL rules that may result to a user role change (that creates a relationship among subjects and objects). User roles are divided to permanent roles (e.g. ambulance nurse) and temporary roles (e.g. attending ambulance nurse). Users are alleviated from the burden to change roles at run time by automatic role changes (e.g. from permanent roles to temporary roles and vice versa) [6]. For example, in emergency healthcare on ambulance selection for an emergency case, the ambulance staff with permanent role "ambulance physician" is granted the temporary role "attending ambulance physician". This is revoked on ambulance arrival at the hospital emergency department ED, that is realized by another service execution. In particular, role change rules were described as follows [6]:

Definition (Role change): A role change is a 4-tuple (u, ri, rj, {pk}) stating that a user u holding the role ri receives the role rj subject to contextual constraints {pk}.

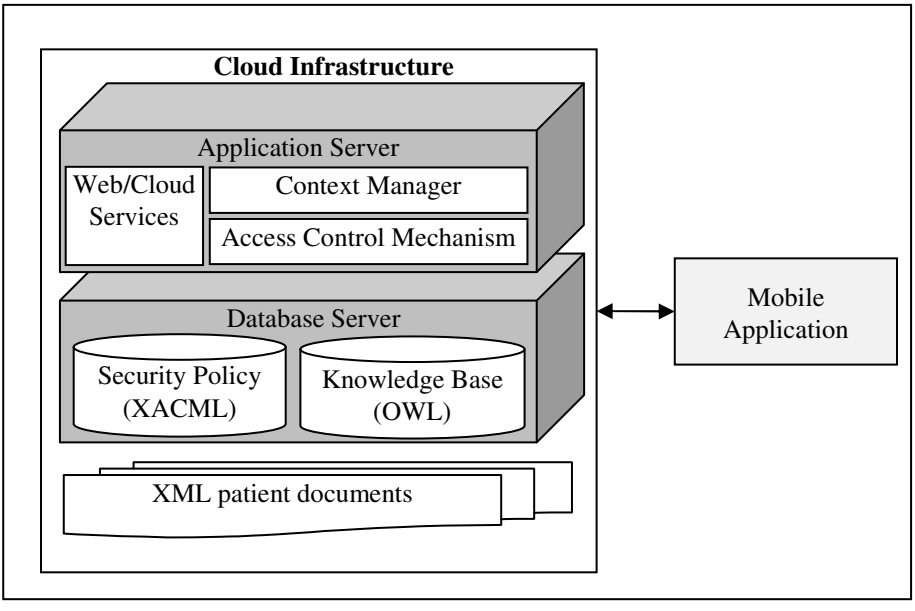

Fig. 1. The proposed access control framework

The role-based access control policy rules specified are evaluated by the ACM according to contextual constraints resulting from the ontology inferring. Those contextual constraints might include authorization delegations that are required when a service S2 invocation is requested after a service S1 execution. Then, the authorization for invoking the S1 should be delegated for the same user role to the S2. This is achieved by sending appropriate context information after S1 execution to the CM. Then, the domain ontology is inferred that result to authorization delegation for S2 invocation. For example the authorization for a service that produces a XML document is delegated to the same user role to enable cloud service invocation for storing this document to the cloud. The access control rules for services invocations and XML document accesses are described as follows [6]:

Definition (web/cloud services invocation): An access control rule for web/cloud service invocation is a 4-tuple (r, "invoke", S, {pk}) stating that a user holding the role r is allowed to invoke web/cloud service S subject to contextual constraints {pk} including authorization delegations.

Definition (XML document access): Given a rule for invoking web/cloud service S by a user holding the role r, an access control rule for XML document access is a 5-tuple (r, "access", S, XML, {pk}) stating that a user holding the role r is allowed to access (read/write) XML document during S execution subject to contextual constraints {pk}.

3 Results

For testing the proposed security framework, a small part of the emergency healthcare process is considered that involve the prehospital care provided by the ambulance service [3]. Figure 3 shows a simplified view of the emergency healthcare process. The activities "Create CDA doc" and "Update CDA doc" have been implemented by two web services developed based on RESTful technology and the other two activities "Store CDA doc" are implemented by the cloud service Amazon S3 for storing the CDA documents created to the cloud servers. The first REST service (CreateCDA) involves the creation of XML Clinical Document Architecture (CDA) based documents with initial emergency case data. The second REST service (UpdateCDA) involves updating the CDA-based documents with emergency case medical data.

The Protégé editor was used for creating the domain ontology and the Jess rule engine for inferring the ontology and SWRL rules. For the access control mechanism the XML Access Control Language (XACML) implementation by Sun Microsystems was used to implement the authorization services on the cloud infrastructure [7]. Authorizations for CDA documents accesses are specified at the level of XML schema. In order to insert the contextual constraints including the authorization delegations to the XACML rules of the XACML policy the attributes of the XACML subjects and resources were used [4].

According to the prototype implementation, on ambulance request context information "new emergency case" is sent to the CM that consults the ontology to retrieve any contextual constraints that are used to form the XACML request send to the ACM. This results to a decision to allow or not the telephone operator of ambulance service to invoke the CreateCDA service to create a CDA document with case data including the selected ambulance and hospital for the case. After service execution the context information "ambulance and hospital selected" is send to the CM that consults the ontology to trigger appropriate (role change) rules for changing the permanent roles (e.g. ambulance nurse) to appropriate temporary roles (e.g. attending ambulance nurse). The same context information results to an authorization delegation in order to allow telephone operator (who executed the CreateCDA service) to invoke Amazon S3 for storing the CDA document.

While at the place of incident or en-route, "attending ambulance nurse" through the mobile application can invoke the UpdateCDA service for updating the CDA document with the medications administered and/or the procedures performed to the case. Hence, context information "update medical data" is sent to the CM that consults the ontology to retrieve any contextual constraints used to form a XACML request send to the ACM in order to allow or not the service invocation. After service execution, the context information "CDA document updated" is sent to the CM that results to an authorization delegation in order to allow attending ambulance nurse (who executed the UpdateCDA service) to invoke Amazon S3 for storing the updated CDA document. Due to lack of space, a more detailed description of this prototype system implementation will be presented elsewhere.

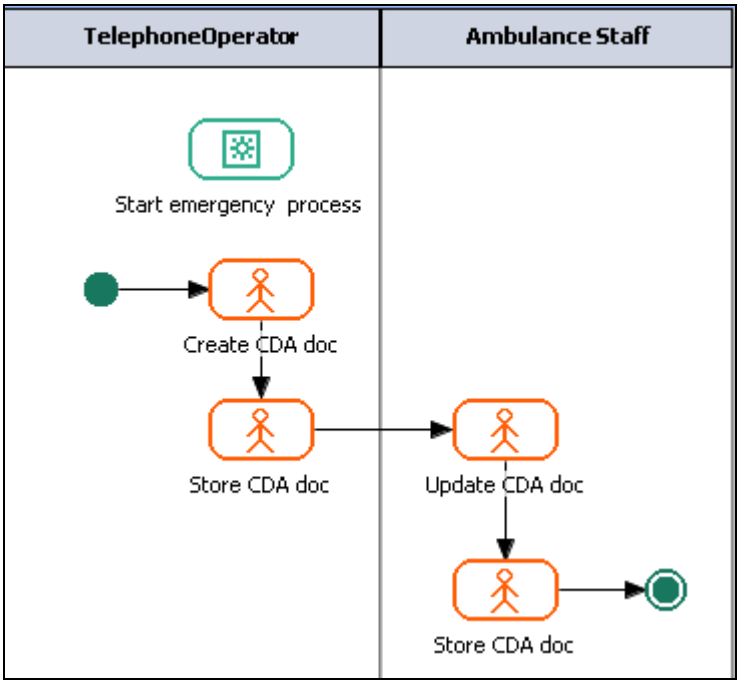

Fig. 2. The emergency healthcare process model designed using Oracle BPM Studio

4 Concluding Remarks

In this paper, is presented an access control framework for providing role-based context-aware authorization services in pervasive healthcare systems that involve the provision of context-aware cloud services to users through their mobile devices. Those authorization services take into consideration the contextual constraints as result from the domain ontology inferring and involve services invocations and XML document accesses. The OWL language is used for representing the domain ontology and SWRL rules were written for expressing role change rules for automatic runtime role changes to users and delegation authorization rules that enables delegating authorizations from a service to another. The prototype system implemented for evaluating the feasibility of the proposed security framework. The rationale behind the envisaged access control framework was to provide users secure access to appropriate services and patient information anytime and anywhere according to context information that represent their changing environment and in a way that the complexity is hidden by the users that is the ultimate goal of pervasive healthcare. Hence, users are alleviated from the burden to change roles manually and authorizations for service executions and patient document accesses are granted to users automatically. However, the proposed framework presented here needs further evaluation in a real world before accepted in a real healthcare environment with adverse circumstances.

References

1. Arnrich, B., Mayora, O., Bardram, J., Troster, G.: Pervasive Healthcare: Paving the Way for a Pervasive, User-centered and Preventive Healthcare Model. Methods Inf. Med. 49(1), 67–73 (2010)
2. Bouzid, Y., Harroud, H., Boulmalf, M., Karmouch, A.: Context-Based Services Discovery in Mobile Environments. In: 16th International Conference on Telecommunications, NJ, USA, pp. 13–18 (2009)
3. Poulymenopoulou, M., Malamateniou, F., Vassilacopoulos, G.: E-EPR: A Cloud-based Architecture of an Electronic Emergency Patient Record. In: 4th International Conference on Pervasive Technologies Related to Assisted Environments, Crete, Greece (2011)
4. Dersingh, A., Liscano, R., Jost, A.: Context-aware Access Control Using Semantic Policies. UbiCC J., Special Issue Autonomous Computing Systems and Applications, 19–32 (2008)
5. Wrona, K., Gomez, L.: Context-aware Security and Secure Context-awareness in Ubiquitous Computing Environments. In: XXI Autumn Meeting of Polish Information Processing Society Conference, Wisla, Poland, pp. 255–265 (2005)
6. Koufi, V., Malamateniou, F., Vassilacopoulos, G., Papakonstantinou, D.: Healthcare System Evolution towards SOA: A Security Perspective. In: 13th World Congress on Medical and Health Informatics, Cape Town, South Africa. Stud. Health Technol. Inform., pp. 874–878 (2010)
7. Zhang, R., Liu, L.: Security Models and Requirements for Healthcare Application Clouds. In: 3rd International Conference on Cloud Computing, Miami, Florida, USA, pp. 268–275 (2010)