IMPLEMENTING SITBAC AS A KNOWLEDGE FRAMEWORK USING OWL AND SWRL

Dizza Beimel
Department of Industrial Engineering and Management,
Ruppin Academic Center,
Emek Hefer, Israel
dizzab@address.ac.il

Mor Peleg
Department of Management Information systems,
University of Haifa,
Israel
peleg.mor@gmail.com

Keywords: Access control, Knowledge framework, OWL, SWRL

INTRODUCTION

In recent years, organizations have been moving from a paper-based to a paper-less state as a result of a computerization process. More and more information is collected, stored and managed in digital form using modern technologies. Some of the data, maintained within an organization's databases, is considered to be *confidential*. For example, *patient health records*, which may hold sensitive information. In such cases, the organization is responsible for establishing a data-access policy in order to maintain confidentiality.

According to the *US Health Insurance Portability and Accountability Act (HIPAA)* [6], which established the first comprehensive federal rule protecting the privacy of health information, **confidentiality** is defined as "the property that data or information is not made available or disclosed to unauthorized persons or processes". In the spirit of this definition, preserving confidentiality involves restricting access to data through authorization and access-control models. One of the leading access-control models is the *Role-Based Access Control (RBAC)* [4]. According to RBAC, authorization to access particular data resources in the organization should be a function of the data requestor's role. One of the advantages of RBAC is its simplicity. However, the model's simplicity turns to be a disadvantage as it limits its expressive power. We have seen this limitation when we conducted a qualitative study to identify real-world scenarios of data-access requests to patients' data [3]. Sometimes, the role prevents medical personnel from accessing data that is required in particular scenarios.

Based on the above, we proposed a different conceptual approach, which enables to formally represent context-based scenarios of data-access within the healthcare domain. The scenarios describe which tasks a data requestor can carry out, with respect to various *contextual factors* (e.g., the location of the data requestor, the status of the patient, and the time of access). Within our model, we structure the scenarios into **Situations**, where Situation is defined as a formal, computer-interpretable representation of a data-access scenario. Thus, by structuring a Situation, we represent an organizational data-access rule. We named our access-control conceptual approach **Situation-Based Access Control**, or **SitBAC** for short [3].SitBAC includes abstractions for modeling the entities involved in data-access scenarios - *Patient*, *Data-Requestor*, *Task*, *Legal-Authorization*, *EHR*, and *Response* - along with their Properties and the Relations among them.

OBJECTIVES

In this abstract, we present **SitBAC knowledge framework**, a formal access-control framework, which is based on the conceptual SitBAC model [3] and enables organizations to define and carry out confidentiality-preserving data-access policies. In particular, we focus on healthcare organizations and health data, stored in electronic health records (EHRs).

METHODS

The idea behind SitBAC knowledge framework is to formally represent the organization's data-access rules as *Situation classes*, and an incoming access-request as an *Individual* (instance) of a Situation class. Within the framework, the individual is mapped into one of the Situation classes in order to infer its appropriate response, i.e., the incoming access-request is either approved or denied. Figure 1 illustrates the above idea.

For that purpose, we chose to base SitBAC knowledge framework on a shared **knowledge model**, or **ontology**. According to [2], an ontology specifies commonly agreed, content-specific definitions for the sharing and reuse of knowledge. Ontologies define a common terminology of the *entities* (concepts) that are assumed to exist in some area of interest, their *attributes*, and the *relationships* that hold among them.

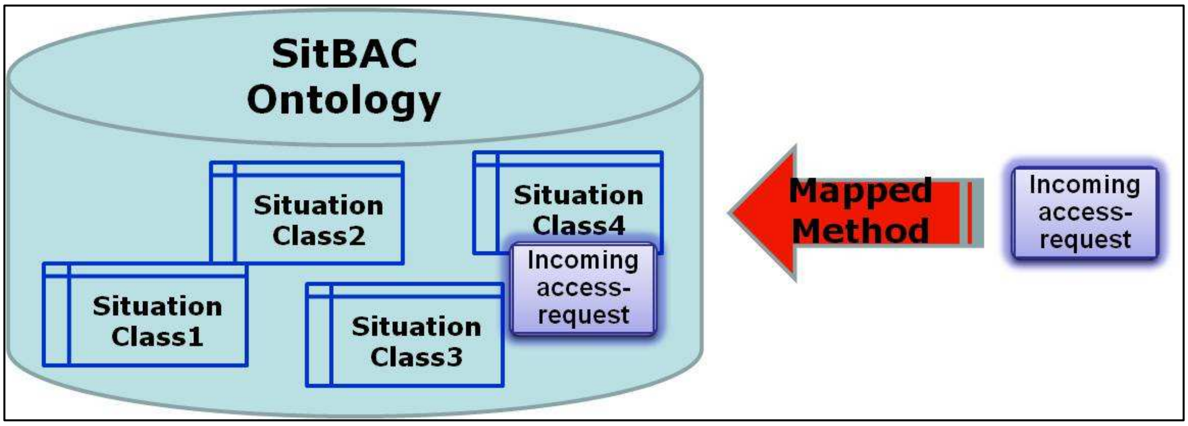

Figure 1: The SitBAC knowledge framework approach

In order to specify the **SitBAC ontology**, we chose the **Web Ontology Language (OWL)** [7] as our ontology representation language, and the *Protégé* knowledge-modeling as our specification tool. The two main reasons for choosing OWL are:

(1) OWL is designed for sharing information over the web, thus, it can be used by a group of healthcare organizations to define and share a common data-access policy by creating a set of *data-access rule classes* (represented via Situation classes).

(2) OWL is a **Description Logics (DL)** [1] language, thus, we can use a description-logics reasoner that provides classification and realization services (as explained in next paragraph).

In our work, we used a DL reasoner to (1) classy the data-access rule classes (Situation classes) and (2) to realize an incoming access-request (represented via an individual of a Situation class) as a member of a data-access rule class, from which the appropriate 'approved/denied' response is inferred.

However, the basic data included in the individual is insufficient and additional knowledge is required in order to accomplish the realization process. To produce the missing knowledge, we used a **Semantic Web Rule Language (SWRL)** [5] engine that inferred the required new facts regarding the individual by chains of properties (e.g., the data requestor's department is equal to the patient's location).

Figure 2 presents the various stages an incoming access-request goes through in order to produce the correct 'approved/denied' response.

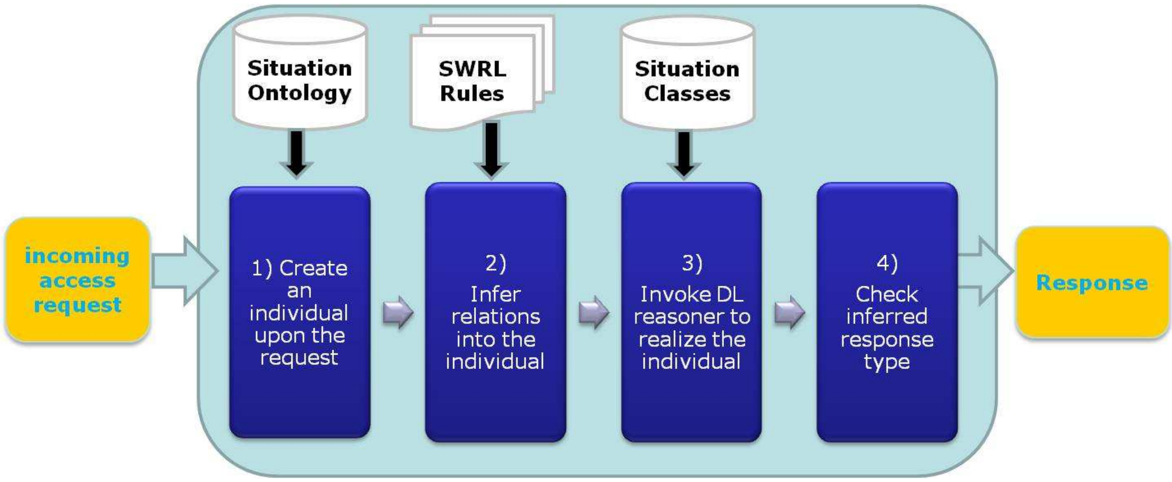

Figure 2. The stages an incoming access request is going through

On top of the above, we designed the SitBAC ontology, including the formal representations for the SitBAC abstractions and the Situation classes, to be *minimal*, *complete*, and *non-conflicting*, taking advantage of ontology exception patterns and using a DL reasoner to discover potential duplications of data-access rule classes.

CONCLUSIONS

In this abstract, we present a context-based access-control framework that aims to support the goal of confidentiality preservation through the use of context attributes and an associated method that operates on them. Our SitBAC knowledge framework is distinct as it (1) is based on a conceptual knowledge model derived from extensive qualitative research which elicited 127 data-access scenarios from the healthcare domain; (2) captures data-access scenarios specific to the healthcare domain and represents the associated context via ontological formalism; and (3) enables the use of a DL reasoner, which is a powerful tool for real-time evaluation of incoming access-requests.

REFERENCES

[1] Baader, F., Calvanese, D., McGuinness, D., Nardi, D., & Patel-Schneider P. (2003). *The Description Logic Handbook*. UK: Cambridge University Press. http://dl.kr.org/.

[2] Gruber, T. (1995). Toward Principles for the Design of Ontologies Used for Knowledge Sharing. *Intl Journal of Human-Computer Studies*, *43*, 907-285.

[3] Peleg, M., Beimel, D., Dori, D., & Denekamp, Y. (2008). Situation-Based Access Control: Privacy Management via Modeling of Patient Data Access Scenarios. *Journal of Biomedical Information*, *41*, 1028-40.

[4] Sandhu, R. S., Coyne, E. J., & Youman, C. E. (1996). Role-based access control models. *IEEE Computer*, *29*, 38–47.

[5] SWRL: A Semantic Web Rule Language Combining OWL and RuleML, http://www.w3.org/Submission/SWRL.

[6] US Depart of Health and Human Services (2003). Summary of the HIPAA privacy rule. http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

[7] Web Ontology Language (OWL), http://www.w3.org/2001/sw/WebOnt/.