IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

XACML Based Solutions for Multiple Environment

Dr. S. Sivasubramanian, S. Geetha, S. Hari Priya

Professor, Computer Science and Engineering, Dhanalakshmi College of Engineering, Chennai, India

Student, Computer Science and Engineering, Dhanalakshmi College of Engineering, Chennai, India

Abstract: Online Collection and Publication of data about individuals may reveal sensitive information about users. In-line with different access scenarios health-Science data is a known example. When searching for information online atomically the Sensitive data may not be revealed but when integrating the data from different web-servers the sensitive information may be revealed. So privacy policy is needed when accessing data online. XACML is a privacy policy language that is used to provide access control to the users by dynamically evaluating rules and Policies.

Keywords: Context, Data, Privacy, Web Service.

I. INTRODUCTION

The main purpose of this project is XACML-based access control to hospital environment. To dynamically evaluate rules to the individual users and to evaluate Policies. Technology advancements facilitate online collection and publication of data about individuals, which is a potentially distributed among several organizations. Each and every organization will manage it's data access and usage through a specialized Web service. In such kind of service oriented interactions, data can be accessed in multiple ways, including manual submission of query through SPARQL endpoints, mash up service APIs with minimal human interaction. Health science data is a known example, where the focus is on transforming the data into ontology-based repositories using RDF (as a universal healthcare exchange language). Each repository defines ontology (in OWL format) of all the concepts that can be searched for in a requester's query. OWL defines classes as a generic concept of individuals and data type properties to link individuals of those classes to the data values. Dynamic service composition will be involved, especially since the queried data may not necessarily get retrieved from a single Web service.

II. EXISTING SYSTEM

Dynamic composition of different data can be misused by the adversaries to reveal sensitive info, which was not deemed by the data owner at the time of data collection. Atomically, these data items may not reveal personally sensitive information of an individual, but when linking those items may lead to some unintended breach of privacy. The problem of privacy management in such services-based interactions raise challenges especially in web browsing, privacy protection need to be performed while the user is looking for data online.

III. PROPOSED SYSTEM

In our proposed project we just build a dynamic, semantic-based privacy policy management framework on the top of the XACML reference architecture for policy-based access control. Context handling in XACML, which is a protocol of communication between a PDP and a Policy Enforcement Point (PEP) (located on the user agent side or on the Web service side, or it is a gateway between the user and the service). The PEP first forms an XACML request and sends it to the PDP through the Context Handler. The PDP then uses those attributes of PEP to evaluate policies. The PDP then requests additional attributes from the context handler as when it is required and finally returns a Permit or Deny decision to the PEP, which enforces the final decision.

Composition plan is generated in which web service1 is depended on other web service. To manage privacy, Web Services define a privacy policy for each instance in the OWL repository. Each repository manages data access through specialized SPARQL endpoint.

IV. OVERALL DESCRIPTION

A. PRODUCT PERSPECTIVE

Dynamic composition of different data will be misused by the adversaries to reveal the sensitive information of an individual, which was not deemed as such by the data owner at the time of data collection. Atomically, these data items may not reveal personally identifiable information, but linking the items together will lead to privacy issues. This problem of privacy management in such Services-based interactions raises challenges specifically in web browsing when the user searches for data online, policy of privacy protection is to be performed when the user is looking for the online data.

Dynamic rule evaluation is not supported in the existing system. Doctors can access the previous year's dataset of hospital for Diagnosis.

B. PRODUCT FEATURES

We just build a dynamic, semantic-based privacy policy framework on the top of the XACML architecture for policy-based access control and we use ontological framework for resource access in repositories for Hospital

DOI 10.17148/IJARCCE.2016.5326

Automation System. Context handling in XACML which is a protocol of communication between a PDP and a Policy Enforcement Point (PEP) (located on the user agent side or on the Web service side, or it is a gateway between the user and the service). The PEP forms and sends an XACML request to the PDP through the Context Handler. The PDP uses the attributes to evaluate policies. The PDP then requests some additional attributes from the context handler as needed and finally returns a Permit or Deny decision to the PEP, which enforces the final decision.

Composition plan will be generated on the basis of access response from XACML and the service dependencies were evaluated (where any service WS1 which depends on another service WS2) to compose web services that will be invoked later sequentially. To manage data privacy, Web Services defines a privacy policy for each instance in its OWL repository. Each repository manages data access through SPARQL endpoint. SPARQL prevents the user request contents to be dispatched to the remote server.

V. EXPERIMENTAL WORK

A.REGISTRATION AND APPOINTMENT

Users in the hospital environment must register at the web end of the registration page. The server then stores the information in the database. Now the patient login and fix appointment to the Doctor by mentioning date and time of the appointment, disease, specialist and doctor name. Each Doctor views their appointment in their appointment page.

B. XACML POLICY FOR RESOURCE ACCESS

Admin set privileges to staff for the data to be accessed from different web services. Staff will be categorized as Doctor, Staff Nurse, and Lab Technician. Each web service has an Ontology repository. Data accessed from Web Service will be classified into three categories: Sensitive, Low Sensitive and High Sensitive. Based on category of the Staff, an XACML Policy will be created by the admin. Dynamic rules can be created in XACML Policy.

C. WEB SERVICE COMPOSITION, DIAGNOSIS AND PATIENT REPORT

Doctor views patient information such as disease, prescription etc. If doctor has a doubt about disease, he/she can contact Research Department to retrieve Medicine or Treatment Type detail. Patient is advised to take lab test. Lab Technician provides test result to patient. If Lab Technician has doubt to deciding lab result, he/she can contact Research Department. XACML Policy will be applied to Lab Technician. Decision to access lab result will be based on Lab Technician XACML Policy. Based on test result, Doctor decides patient type: In Patient or Out Patient.

D. HOSPITAL AUTOMATION AND BILLING

Out Patient Information will be sent to Patient Page. Patient Page contains hospital fees to be paid including lab fees, doctor fees etc. Patient will be redirected to Bank to pay fees. After successful transaction, Patient Report will be generated. If the Patient type is In Patient, Doctor sends report to Staff Nurse. If Staff Nurse views attributes, access decision check occurs in PEP and PDP. If the access is Permit, Staff Nurse can view otherwise not. If the Patient is discharged from hospital, he/she will be redirected to Bank to pay fees. After successful transaction, Patient Report will be generated.

VI. TECHNIQUES

A.XACML FRAMEWORK

The most widely used privacy policy language is XACML which is also preferred for privacy. According to standard XACML-based privacy policy management model, the organization which hosts the Web service should first define a policy administration point (PAP), from which policies can be defined and further it is deployed to a Policy Decision Point (PDP). Context handling a task in XACML is a protocol of communication, between a PDP and PEP (located on user agent side or the Web service side, or it is a gateway between the user and the service). The PEP first form an XACML request and sends it to the PDP through the Context Handler, which collects the attributes from policy Information points (PIP). The PDP then uses the attributes to evaluate the policies. The PDP then requests some additional attributes from context handler as it needed and finally returns a Permit or Deny decision to the PEP, which enforces the final decision.

B.QUERY BASED TECHNIQUE

The query based technique is used to get relevant data for an input query from the database.

Steps:

1. Input query.
2. Retrieve data from Database based on Query.

VII. DESIGN AND IMPLEMENTATION CONSTRAINTS

A.CONSTRAINTS IN THE ANALYSIS

1. As Informal Text
2. As Operational Restrictions
3. Constraints that is Integrated in Existing Model Concepts
4. As a Separate Concept
5. Constraints that is Implied by the Model Structure

B. CONSTRAINTS IN THE DESIGN

1. Determination of Involved Classes
2. Determination of Involved Objects
3. Determination of Involved Actions
4. Determination of Require Clauses
5. Global actions and its Realization constraint

C. CONSTRAINTS IN THE IMPLEMENTATION

A hierarchical structure of relations can result in more number classes and it will be of more complicated structure which is difficult to implement. Therefore it is advisable to transform those hierarchical relation structures to a simpler one such as a classical flat one. It is straightforward to transform those developed hierarchical model to a bipartite, flat model, that consisting of classes on the one hand and flat relations on the other one. Flat

DOI 10.17148/IJARCCE.2016.5326

relation is preferred for design level for reasons of simplicity and implementation easy. There will be no identity or any functionality associated in a flat relation. A flat relation corresponds to the relation concept of entity-relationship(ER) modeling and many object oriented methods.

VIII. ENHANCEMENTS

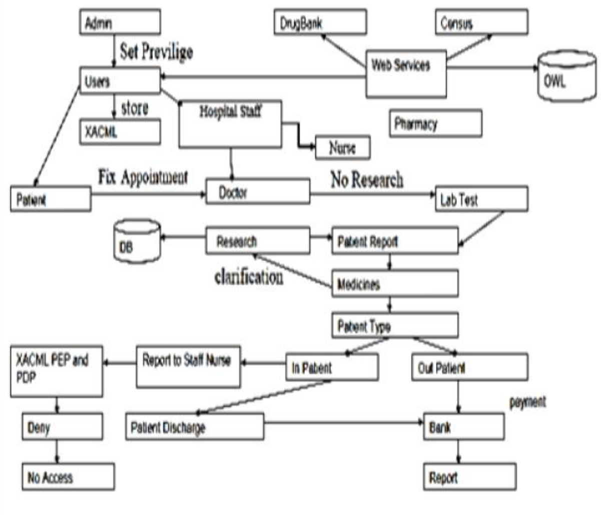
A.BANK SERVICE

Out Patient Information will be sent to Patient Page. Patient Page contains hospital fees to be paid including lab fees, doctor fees etc. Patient will be redirected to Bank to pay fees. After successful transaction, Patient Report will be generated. If the Patient type is In Patient, Doctor sends report to Staff Nurse. If Staff Nurse view attributes, access decision check in PEP and PDP. If the access is Permit, Staff Nurse can view otherwise not. If the Patient is discharged from hospital, he/she will be redirected to Bank to pay fees. After successful transaction, Patient Report will be generated.

B. XACML FRAMEWORK IS IMPLEMENTED FOR HOSPITAL AUTOMATION

XACML framework is implemented for the hospital Environment. Access controls are set to the users in the hospital Environment. Based on the policy the users are allowed to access information. Privacy policy is provided to the users.

IX. FIG. XACML BASED INTERACTION IN DYNAMIC ENVIRONMENT



XACML BASED INTERACTION IN DYNAMIC ENVIRONMENT

X. ABBREVIATIONS AND ACRONYMS

XACML- eXtensible Access Control Markup Language
PEP – Policy Enforcement Point
PDP – Policy Decision Point
PAP – Policy Administration Point
PIP – Policy Information Point
OWL – Web Based Ontology Language
RDF – Resource Description Framework

XI. CONCLUSION

XACML privacy policy management framework is implemented in collaborative service-based data sharing health environment. This framework provides dynamic evaluation of rules and decision enforcement.

REFERENCES

1. B. Franc¸ois, M.-A. Nolin, N. Tourigny, P. Rigault, and J. Morissette, “Bio2RDF: towards a mashup to build bioinformatics knowledge systems,” J. biomedical informatics, vol. 41,no. 5, pp. 706–716, 2008.
2. EHealth Information Platforms (EHIP). [Online]. Available: http:// distrinet.cs.kuleuven.be/ research/projects/EHIP, Dec. 2013
3. Axiomatics Language for Authorization (ALFA). [Online]. Available: http://www.axiomatics.com/solutions/products/authorization-for-applications/developer-tools-and-apis/192-axiomatics-language-for-authorization-alfa.html
4. Sun’s XACML Implementation. [Online]. Available: http://sunxacml.sourceforge.net/, 2003.
5. WSO2 Balana Implementation. [Online]. Available: https://github.com/wso2/balana, 2013.
6. D. Agrawal and C. C. Aggarwal, “On the design and quantification of privacy preserving data mining algorithms,” in Proc. SIGMOD-SIGACT-SIGART Symp. Principles Database Syst., 2001,pp. 247–255.
7. R. Agrawal and C. Johnson, “Securing electronic health records without impeding the flow of information,” Int. J. Med. Inf.,vol. 76, pp. 471–479, 2007.
8. Ching Hsu Department of Computer Science and Information Engineering, National Formosa University, 64, Wenhua Rd., Huwei Township, Yunlin County 632, Taiwan “Extensible access control markup language integrated with Semantic Web technologies”
9. M. Barhamgi, D. Benslimane, C. Ghedira, and A. L. Gancarski, “Privacy-preserving data mashup,” in Proc. Int. Conf. Adv. Inf. Netw. Appl., 2011, pp. 467–474.
10. R. Bhatti, E. Bertino, and A. Ghafoor, “A trust-based context aware access control model for web-services,” in Proc. Int. Conf.Web Services, 2004, pp. 184–191.

DOI 10.17148/IJARCCE.2016.5326