Privacy-Aware Smart Learning: Providing XACML as a Service in Semantic Web based Smart Environment

Isma Farah Siddiqui and Scott Uk-Jin Lee
Department of Computer Science and Engineering, Hanyang University
Ansan, South Korea
[e-mail: isma2012@hanyang.ac.kr, scottlee@hanyang.ac.kr]
*Corresponding author: Scott Uk-Jin Lee

Abstract

Smart environment when integrates with semantic web provides context-awareness to processed information. To this end, smart solutions have adopted self-learning techniques as an integral part for efficient retrieval of data. Many smart solutions are being deployed with privacy parameters but lacks with in-place privacy approach over processed information. To overcome this issue, we present a novel approach of applying X_{ACML}aaS (XACML as a Service) in a semantic web based smart environment. The proposed framework targets fine grain access control authorization over heterogeneous data captured from smart IoT devices and sensors. This paper also highlights the prototype implementation of access control as a service with a preliminary use case scenario of smart education environment.

Keywords: Smart Learning, Access Control, Context-Aware Smart Environment, Semantic Web

1. Introduction

Emergence of smart sensors and devices introduced paradigm of pervasive computing which provide Ambient Intelligence (AmI) to physically connected devices i.e. Internet of Things (IoT). Semantic web technologies (OWL, RDF, and SPARQL) in AmI environments allows flexibility to utilize currently available smart IoT devices. XACML (eXtensible Access Control Markup Language) is an XML based language for access control [1]. The architecture of XACML can incorporate access control solutions as Attribute based access control (ABAC), Role Based Access Control (RBAC) or Policy based Access Control (PBAC). Due to dispersed availability, smart environments are unable to focus procedural deployment of XACML policies with in-place authorization approach.

Various researchers worked on providing information security, specifically with authorized access control on cloud platforms. However, up to our vision none of them works for ensuring access control authorization over semantic web based smart environment. Researchers in [2] and [3], exploited the use of ontologies to model context information for machine learning over IoT, However, did not highlighted any aspect of privacy. Cadenhead et al. [4] gave approach of access control security over RDF graphs. Some of the researchers considered security based works on smart environment. SAFIR [5], gave a comprehensive approach in dealing with smart city data security, user privacy and trust issues. Alfredo et al. [6] gave idea of access control at triple level.

This work was supported by the ICT R&D program of MSIP/IITP. [12221-14-1005, Software Platform for ICT Equipments]

However, their approach did not considered application with smart environment. Khadilkar et al. [7] have given a detailed study of information sharing and privacy in private clouds using XACML and semantic web, but not applicable over smart environments because of processing overhead of ontology based information. In this research we gave an innovative approach to exploit semantic information obtained from physical IoT devices and ensuring privacy using access control authorization as a service. With authorized accessibility, semantic information provides assistance to control connected smart devices and supports to perform decisive tasks on behalf of users.

In this paper, we present a novel approach of using XACMLaaS in a smart environment with embedded semantic web technologies for secure context-awareness. The proposed prototype shows use of security and privacy as an in-place dependent component in a service layer. The main contributions of this papers are:

- A novel approach to integrate security and privacy layer within a semantic web based smart environment.
- Inter-operative data filter procedure with an independent XACML policy management.
- Reusability of policy enforcement mechanism between access control service, user interface and application server layers.

In rest of this paper, section 2 shows insight of our novel approach of using XACMLaaS in a semantic web based smart environment along with details of framework architecture. Section 3 discusses a smart education environment as a motivating scenario for implementation of proposed framework. Finally, section 4 concludes the paper and provides future directions.

2. XACML as a Service in Semantic Web based Smart Environment

2.1 Context-awareness using Ontology

Semantic web techniques represents data as RDF for machine interpretation. The semantics are provided with ontology annotations using OWL, which offers effective information management and sharing within a smart environment. Data obtained from smart devices complies with associated ontology and structured as RDF for context-aware decision support.

2.2 Access Control as a Service

The proposed architecture for utilizing access control as a service layer is based on semantic web techniques over structured data from IoT. This approach ensures privacy by means of access control authorization while accessing environment resources. The access control service layer acts as an independent entity along with smart environment component layers. Access control authorization is provided by XACML, which supports implementations for RBAC, ABAC and PBAC models and also incorporates fine grained authorization. These models over semantic cloud fulfills the demand for on-site and required access control enforcement strategies. With device level, policy based and attributes based access control are acceptable, whereas for different types of users, role based authorization is more applicable.

Fig. 1 shows the work flow of access control service layer. The access control service layer describes the key components of XACML access control authorization, as: (1) Policy Information Point (PIP), (2) Policy Decision Point (PDP), (3) Policy Enforcement Point (PEP) and, (4) Environment Attributes and User/Role Store.

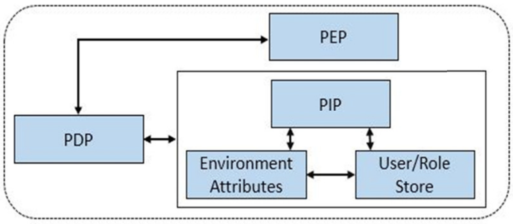

Fig. 1. XACMLaaS Data flow Diagram

1) Policy Information Point (PIP): serves as a source of attribute values. If there are missing attributes in the XACML request sent from PEP, then PIP would identify them for the PDP to evaluate the policy.

2) Policy Decision Point (PDP): evaluates a policy applicability over a resource and returns an authorization decision to the PEP. In order to process PDP, set of rules are to be considered to make certain decision.

3) Policy Enforcement Point (PEP): performs access control authorization by working over decision requests and enforcing policy decisions for authorized access to a resource.

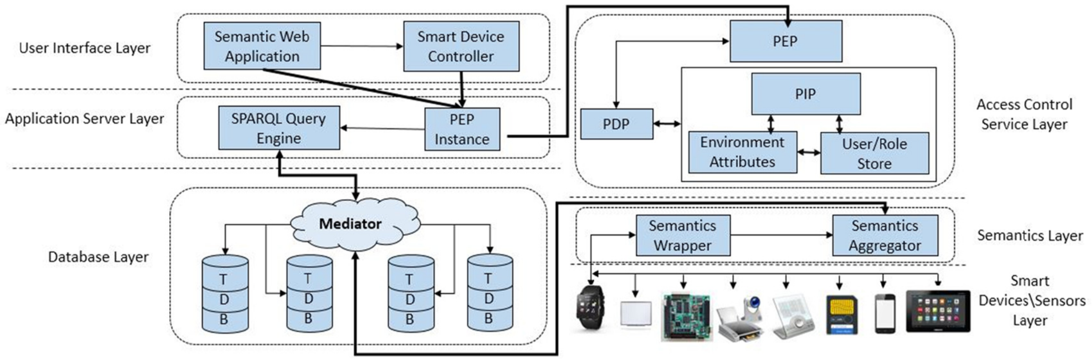

Fig. 2. Access Control as a Service in Semantic Web Based Smart Environment

All rulings from PDP are enforced by PEP based on filters for decision of pass or fail the request further to SPARQL query engine for further query processing.

4) Environment Attributes and User/Role Store: acts a secondary entities for storing information about attributes, users, roles and groups.

2.3 Layered Framework of Semantic Web based Smart Environment

An overall framework for semantic web based smart environment is illustrated in Fig. 2, which shows multiple layers for information processing.

1) Semantics Layer:
Semantics Wrapper
Semantics wrapper is a software component for mapping raw data from smart devices and formatting it into meaningful. The wrapper obtains data from smart devices applications such as notification status of device, location information and temperature measurements using GPS and Google Maps etc. The mapped RDF data is forwarded to semantic aggregator.
Semantics Aggregator
This component gathers RDF triples and has the capability to aggregate different triples and store as new triples in the triple database. The aggregator is also responsible to generate rule based triples with re-gathering and merging values from existing triples.

2) Database Layer:
Triple Database(TDB) Stores and Mediator
The RDF triples are stored in a TDB and Mediator is responsible to implement higher level services for synchronization to avoid race conditions and deadlock.
3) Access Control Service Layer:
This layer is responsible to enforce authorization as a service for ensuring privacy of information. The PEP module receives SPARQL query request from end user application and authenticates the role of user after it receives authorization decisions from PDP. The PDP evaluates the authorization decision for resource attribute and return it to PEP.

4) Application Server Layer:
SPARQL Query Engine
The triples from TDB are queried using SPARQL queries. The query engine acts as a HTTP local host server and supports to give access to query endpoints using RESTful services. The server layer can host multiple query engines to support distributed smart environment.
PEP (Policy Enforcement Point) Instance
The instance of PEP is hosted over server and query request made from user interface layer is directed towards this module for user authentication and authorization. In distributed smart environment, there can exist multiple instances of PEP for concurrent access control.

5) User Interface Layer:
Semantic Web Application
The semantic web application is accessed by end users. It accepts SPARQL query and forward it to query engine. The exclusive set of users for this application ranges among different user groups or roles, to provide fine-grained data accessibility. Permission to process query is provided after permit decision is evaluated at PEP from access control service layer. The permission is then forwarded to query engine which further perform processing for accessing

RDF triples from TDB.

Smart Device Controller Application
The smart device controller application enforce event-based actions or timebased queries using query engine. Using the obtained RDF results, it generates rule-based decisive commands for smart devices, and manage behavior of connected smart sensors and devices.

3. SWSEE: A Use Case Scenario

In order to present the feasibility of utilizing XACMLaaS in smart environment, we present transition of smart education environment to Semantic Web based Smart Education Environment (SWSEE). The principal working domains of SWSEE are illustrated in **Fig. 3**. Traditionally smart education environment enables data sharing among different connected devices through web services via Internet and mobile communication. However, proposed SWSEE aims to share information semantically in RDF format and enables AmI using semantic web REST-full services. The layered architecture of X_{ACML}aaS when applied over SWSEE would be practiced by a semantic web application whose targeted role audience broadly includes: teacher, student and administrative staff.

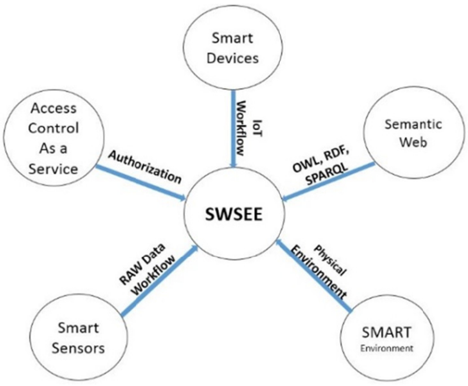

Fig. 3. Scope of SWSEE

4. Conclusions

In this paper, we have presented an access control policy language based privacy service for securing information over smart environment. X_{ACML}aaS uses semantic web techniques with XACML language over a formatted group of policy layer components. Our proposed framework shows efficient adaptation of XACML as a service in smart environment. This innovative research provides a context-aware secure information accessibility, rule based decision making and reasoning capabilities to manage smart sensors and devices on behalf of user. In future, we plan to fully integrate proposed service with group of inter-operative cloud services to formulate a heterogeneous semantic web based smart environment.

References

[1] B. Parducci, H. Lockhart, R. Levinson, and M. McRae, "Extensible access control markup language–version 2.0," OASIS Standard, 2005.

[2] K. Maria, E. Vasilis, and A. Grigoris, "S-CRETA: Smart classroom real-time assistance," in *Ambient Intelligence-Software and Applications*. Springer, 2012, pp. 67-74.

[3] J.-P. S. Esa Viljamaa, Jussi Kiljander and A. Ylisaukko-oja, "A smart control system solution based on semantic web and uID," in *Proc. Of Fifth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM)* pp. 105-110, 2011.

[4] T. Cadenhead, M. Kantarcioglu, V. Khadilkar, and B. Thuraisingham, "Design and implementation of a cloud-based assured information sharing system," in *Computer Network Security*. Springer Berlin Heidelberg, pp. 36-50, 2012

[5] J. L. Hernández-Ramos, M. V. Moreno, J. B. Bernabé , D. G. Carrillo, A. F. Skarmeta, "SAFIR: Secure access framework for IoT-enabled services on smart buildings," *Journal of Computer and System Sciences*, Vol 81, No. 8, pp. 1452-1463, 2014.

[6] A. D'Elia, J. Honkola, D. Manzaroli, and T. S. Cinotti, "Access control at triple level: Specification and enforcement of a simple RDF model to support concurrent applications in smart environments," in *Smart Spaces and Next Generation Wired/Wireless Networking*. Springer, Vol 6869, 2011, pp 63-74, 2011.

[7] V. Khadilkar, T. Cadenhead, M. Kantarcioglu, and B. Thuraisingham, "Assured information sharing (AIS) using

private clouds," in *High Performance Cloud Auditing and Applications*. Springer New York, pp. 215-255, 2014.