ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

Smart Hospital Management System

Hemina Joy Fernando S, Kallagunta Venkata Amulyasree, Swathi J

hemina_fernanado@yahoo.com amulyasree6@gmail.com swathinair261@gmail.com

CSE Department, KCG college of Technology

Chennai-97

Under the Guidance of

Mr Sankar S

Associate Professor, CSE Department

KCG College of Technology

Chennai-97

Abstract— **The Paper aims at developing a Web-Service based Hospital Management System by enforcing XACML-based access control and Dynamic rule evaluation and decision enforcement. Using this technology Patients, Doctors and every Staff personnel of the Hospital are registered into the system. The patients can thereafter login to the Web-service and fix appointments with the available doctors, make online payment, retrieve their report from the online web-service in pdf format. The Doctors can login and view their appointments, add fee details, forward any patient-id for specific lab tests, can make use of resources from research department etc. Likewise the Lab Technicians, Staff Nurse can login and view the received lab test requests, forward the results directly to the doctor. The above mentioned functionalities are rendered as a composition of Web-Services.**

Technology advancements facilitate the online collection and publication of data about individuals, which could potentially be distributed among several organizations (e.g., testing labs, research institutes, etc.). In line with the different access scenarios, health science data is a prime example. Dynamic service composition may be involved, especially since the queried data may not necessarily get retrieved from a single Web service. Hence XACML framework is used to formulate and manage the Privacy policy of the data handled in this automation system.

***Keywords*— Hospital Management, XACML framework, privacy policy, Hospital Automation**

1. INTRODUCTION

Technology advancements facilitate the online collection and publication of data about individuals, which could potentially be distributed among several organizations (e.g., testing labs, research institutes, etc.). Each organization may manage its data access and usage through a specialized Web service. In such services based interactions, data can be accessed in several ways, including manual query submission through SPARQL endpoints, automated analysis pipelines and scientific workflows, and mash up service APIs with minimal human interaction. In line with the different access scenarios, health science data is a prime example, where the focus has been 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 (e.g., Patient) and data type properties to link individuals of those classes to their data values. Dynamic service composition may be involved, especially since the queried data may not necessarily get retrieved from a single Web service.

2. EXISTING SYSTEM

Dynamic composition of different data items (retrieved through participating Web services) may be misused by adversaries to reveal sensitive information, 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 those items may lead to unintended breach of privacy. The problem of privacy management in Services-based interactions raises challenges especially since in web browsing, privacy protection need to be performed while the user is looking for data online. Existing System access control does not support dynamic rule evaluation. Doctors can access the previous year's dataset of hospital for Diagnosis.

3. PROBLEM DEFINITION

A Hospital environment may suffer from some of the privacy issues: sensitive information from different data items (retrieved through participating Web services) can be misused by adversary. Linking of data items lead to an unintended breach of privacy. So, Access Control is necessary in this environment.

4. PROPOSED SYSTEM

A dynamic, semantic-based privacy policy management framework on the top of the XACML reference architecture for policy based access control is built and ontological framework for resource access in repositories for Hospital Automation System is used. Context handling is a protocol of communication between a PDP and a Policy. Enforcement Point (PEP) (located either on the user agent side, the Web service side, or on a gateway between the user and the service). The PEP forms an request and sends it to the

PDP through the Context Handler. The PDP then uses those attributes to evaluate policies. The PDP requests 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 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.

5. RELATED WORK

We discuss some of the existing approaches for privacy policy management.

5.1 Context Awareness The literature has several works that have proposed context-aware privacy management systems. Some of these approaches dynamically handle a user request by applying techniques that regulate rather than prevent the data access such as HDB. The dynamic trust adjustment model proposed in also dynamically handles context, but they focus on access control, in terms of who has access to the information as opposed to what is being collected. Also, their approach relies on inferring context using sensed spatial and temporal information and they do not achieve dynamicity at rule level. Several technologies have been applied to achieve privacy policy enforcement by considering the requester's permission, the owner's consent, and the context. Grandison and Agarwal[6] leverage the Active Enforcement module of the Hippocratic Database (HDB) technology by transforming an original query to another query that is policy compliant. Similar to our approach, those approaches do not rely on a third party for enforcement purposes. They also track the purpose of a query to determine if a query is suspicious or not, but do not keep track of usage context

5.2 Dynamic Rule Evaluation Few researchers have started looking at dynamic policy rule evaluation as opposed to static policies. Among the relatively few researchers who took dynamicity of a context to a higher level by considering dynamicity of a rule is Pallapa et al. They proposed a context aware scheme for privacy preservation by maintaining a model of the user's environment, which is characterized by user's activities and situations. Their solution accounts for fine grained rules and they apply a dynamic rule generator. However, both the rule and the context types are still predetermined based on a set of activities and states in which the user could be. Also, these rules are not defined in semantic terms and do not govern what is potentially sensitive data. Our approach implicitly updates policy rules based on dynamically inferring a query's classification, what is considered relatively sensitive data, and diversity of queries. Christo Ananth et al. [3] discussed about an eye blinking sensor. Nowadays heart attack patients are increasing day by day."Though it is tough to save the heart attack patients, we life of others whom they are responsible for. The main design of this project is to track the heart attack of patients who are suffering from any attacks during driving and send them a medical need & thereby to stop the vehicle to ensure that the persons along them are safe from accident. Here, an eye blinking sensor is used to sense the blinking of the eye. spO2 sensor checks the pulse rate of the patient. Both are connected to micro controller.If eye blinking gets stopped then the signal is sent to the controller to make an alarm through the buffer. If spO2 sensor senses a variation in pulse or low oxygen content in blood, it may results in heart failure and therefore the controller stops the motor of the vehicle. Then Tarang F4 transmitter is used to send the vehicle number & the mobile number of the patient to a nearest medical station within 25 km for medical aid. The pulse rate monitored via LCD .

5.3 Relative Sensitivity Some notable techniques that applied machine learning, data mining, or information theory for sensitive data detection. Agarwal et al.[6] have done valuable work in that respect. In their work they defined conditional privacy using conditional entropy and information loss. We leverage similar techniques to partially define our context. Our approach for sensitive data detection is complementary to other approaches. Machanavajjhala and Gehrke have proposed the notion of perfect privacy using query containment mapping to ensure perfect privacy for relational data. Based on that, Barhamji et al. developed a query rewriting approach for data mash up services and applied it to RDF views.

5.4 XACML Enhancements Several researchers have provided enhancements to the performance of XACML[4] PEP and PDP components, such as efficiency and scalability and adaptation but there exist very few works that have provided enhancements to the accuracy of the PEP by enhancing the context handler, which is the essence of our approach. Laborde et al. have recently implemented self-adaptive authorization frameworks based on XACML that improves the accuracy of PEP by tracking malicious behaviours. Brucker and Petritsch enhanced the context handling protocol used in XACML, but they focus on the efficiency of attribute resolution strategie's either via the PIP or the XACML context handler.

5.5 Dynamic Private Data Publishing Privacy preserving data publishing approaches can be classified into two major categories: data disclosure and anonymization. Our approach falls under the limited disclosure category. One representative approach in this regard is Hippocratic databases technology, which enforces privacy at the database level rather than the application level. While they do dynamic privacy disclosure at the cell, column, and row levels, they do not incorporate previously inferred context into future query evaluation. Anonymization techniques can be further classified into generalization and suppression techniques. Several researchers have provided practical implementations of these algorithms ranging from top-down versus bottom-up to global versus local to optimal versus greedy to hierarchy-based versus partition based. All these algorithms prevent uniquely identifying individuals through record linking, but do not prevent sensitive attribute disclosure. L-diversity alleviates this problem by ensuring that sensitive attribute values in each equivalent class are diverse. However, it is possible to infer sensitive attributes when the distribution in a class is very different from the overall distribution of the same attribute. T-closeness, on the other hand, considers the sensitive attribute distribution in each class, and its distance to the overall attribute distribution. The distance is measured using similarity scores for distributions. LKC Privacy provides a generalization over the aforementioned approaches with more reasonable constraints on parameters. In essence, the main drawback to all generalization and suppression algorithms lie in the utility or information loss incurred. Since these approaches rely on frequency of an item, in some cases, certain co-occurrences of items are considered the source of utility especially when record linkage is performed.

6. CONCLUSION

We provided a privacy based hospital environment using a XACML-based implementation of a semantic-based privacy management framework that incorporates context into dynamic rule evaluation and decision enforcement. Our evaluation of the current implementation suggests that the overhead introduced by both the context and semantic handlers does not significantly affect the throughput and evaluation time of a standard XACML-based framework. Our future work includes addressing other issues that service-oriented environments entail. We hope that future enhancements on the current implementation of the proposed model will serve as a foundation for modern health records infrastructures and inspire productive research in information sharing and management.

REFERENCES

[1] 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.

[2] 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.

[3] Christo Ananth, S.Shafiqa Shalaysha, M.Vaishnavi, J.Sasi Rabiyathul Sabena, A.P.L.Sangeetha, M.Santhi, "Realtime Monitoring Of Cardiac Patients At Distance Using Tarang Communication", International Journal of Innovative Research in Engineering & Science (IJIRES), Volume 9, Issue 3, September 2014, pp-15-20

[4] Axiomatic 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.

[5] M. Barhamgi, D. Benslimane, C. Ghedira, and A. L. Gancarski, "Privacy-preserving data mash up," in Proc. Int. Conf. Adv. Inf. Newt. Appl., 2011, pp. 467–474.

[6] 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.

[7] EHealth Information Platforms (EHIP). [Online]. Available: http:// distrinet.cs.kuleuven.be/ research/projects/EHIP, Dec. 2013

[8] B. Franc¸ois, M.-A. Nolin, N. Tourigny, P. Rigault, and J. Morissette, "Bio2RDF: towards a mash up to build bioinformatics knowledge systems," J. biomedical informatics, vol. 41, no. 5, pp. 706–716, 2008.

[9] Sun's XACML Implementation. [Online]. Available: http:// sunxacml.sourceforge.net/, 2003.

[10] WSO2 Balana Implementation. [Online]. Available: https:// github.com/wso2/balana, 2013.

ACKNOWLEDGMENT

We thank the Almighty GOD for the abundant blessings showered on us. We extend our deepest love and gratitude to our dear parents who built up our career and backed us up in life.

We thank our management and our Principal **Dr T Rengaraja M.E, Ph.D.** for the opportunities given to us for our career development.

We feel indebted to the Head of the Department **Mr S. Cloudin M.E,** Department of Computer Science and Engineering, KCG College of Technology, for all his encouragement.

We express our deepest gratitude to the internal guide **Mr S Sankar M.E.,** Associate Professor, Department of Computer Science and Engineering, KCG College of Technology, for his valuable guidance, ideas and support.

We would like to thank all other faculty members of Department of Computer Science for their help and advice to present this paper

Finally, we are thankful to all our friends and all others who encouraged us and helped us in preparing for this paper.