Journal of King Saud University – Computer and Information Sciences (2017) 29, 505–519

King Saud University

Journal of King Saud University – Computer and Information Sciences

www.ksu.edu.sa
www.sciencedirect.com

Proposing hierarchy-similarity based access control framework: A multilevel Electronic Health Record data sharing approach for interoperable environment

Shalini Bhartiya [a,*], Deepti Mehrotra [a], Anup Girdhar [b]

[a] Amity School of Engineering and Technology, Amity University, Uttar Pradesh Sector 125, Noida, U.P., India
[b] Sedulity Solutions, 310 Suneja Towers-II, Janakpuri, New Delhi, India

Received 16 May 2015; revised 16 July 2015; accepted 25 August 2015
Available online 2 November 2015

KEYWORDS

Access control policies;
Electronic Health Records (EHR);
Hierarchical Similarity Analyzer (HSA);
Interoperable healthcare environment;
Security

Abstract Interoperability in healthcare environment deals with sharing of patient's Electronic Health Records (EHR) with fellow professionals in inter as well as intra departments or organizations. Healthcare environment experiences frequent shifting of doctors, paramedical staff in inter as well as intra departments or hospitals. The system exhibits dynamic attributes of users and resources managed through access control policies defined for that environment. Rules obtained on merging of such policies often generate policy-conflicts thereby resulting in undue data leakages to unintended users. This paper proposes an access control framework that applies a Hierarchy Similarity Analyzer (HSA) on the policies need to be merged. It calculates a Security_Level (SL) and assigns it to the users sharing data. The SL determines the authorized amount of data that can be shared on successful collaboration of two policies. The proposed framework allows integration of independent policies and identifies the possible policy-conflicts arising due to attribute disparities in defined rules. The framework is implemented on XACML policies and compared with other access models designed using centralized and decentralized approaches. Conditional constraints and properties are defined that generate policy-conflicts as prevalent in the policies.

* Corresponding author at: ED-94, Tagore Garden, New Delhi 110027, India
E-mail addresses: shalinibhartiya69@gmail.com (S. Bhartiya), mehdeepti@gmail.com (D. Mehrotra), anup@sedulitygroups.com (A. Girdhar).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

1. Introduction

Healthcare is a time-bound service. The major advantage of electronic health care record is timely availability of health data at any desired location so that patient can get appropriate treatment. Along with timely retrieval of health data, equally important is the assurance of maintaining the confidentiality and privacy of patient's health records. This is more complex

http://dx.doi.org/10.1016/j.jksuci.2015.08.005
1319-1578

for health environment primary due to frequent shift of roles, departments and duties. Today is an era of distributed computing (Xiao et al., 2009) where users of different organizations need to collaborate and access each other's resources. Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule of 1996 establishes guidelines for strengthening the privacy and security protections for individual's Electronic Health Records(EHRs) in such collaborations.

An interoperable health system facilitates use of software applications for exchanging data by maintaining many-to-many relationship between health care provider, patients and data resources. This approach provide better integration and sharing but also demand a framework that ensures privacy and security which can be achieved by designing proper policies for the disclosure and use of health care information. Achieving interoperability in an open and dynamic healthcare environment is a difficult task (Bhartiya and Mehrotra, 2013) and requires a cooperative access control approach to achieve secured sharing of authorized data to the users. Traditional access control framework varies between centralized to decentralized access control approaches and for sharing of EHR among different organization, access for secured sharing can be controlled and managed either through centralized or decentralized approach.

The centralized access control approach (Carmagnola et al., 2000) relies on a central authority for permitting/denying access to the required resources. It results in consistent and uniform supply of data to the legitimate users. The centralized control of access reduces administrative effort of managing the resources but also is vulnerable in terms of security threats. Usually in an interoperable environment, it is not possible to design a centralized access control model. A need exist to design an authorization system (NIST SP 800–162) in order to maintain proper integrity, confidentiality and availability of the data. Decentralized approach (Saltman et al., 2007) distributes the authority to the person nearer to the resource. Each decentralized system has its own conceptual storage and hierarchies of users and resources. The powers of permitting/denying access to the data are distributed to each person who leads one or more team in an organization. This approach is the most sought in ubiquitous computing environments directly exchanging data in peer-to-peer manner. This model lacks consistency controls but ensures quick access to data and other resources.

Accessing data in interoperable environment also experiences contradictory or undefined authorizations necessary for administering the accountability on sharing of data between disparate systems. Another relevant issue while integrating disparate access control policies is the emergence of policy-conflicts where two or more rule may contradict with each other. Information sharing in healthcare environment is usually dynamic. It requires preserving the availability, integrity and confidentiality of EHRs that may differ with each patient's need.

A framework proposed in this paper considers Attribute based access model (ABAC) as its base model. Attribute based access model (ABAC) (Hu et al., 2013) is a logical access control methodology where rule attributes are evaluated to determine the authorization for performing the set of defined operations. The idea is to fine-grain the available access control policies on the basis of the user's hierarchical positions in their respective organizations. It requires designing of framework that follows the principles of least privilege ensuring generation of only the relevant rules. Due consideration is given to preserve the internal consistency and authorization while refining the given policies.

This paper is divided into 6 sections. Section 1 explains the need and significance of interoperable healthcare environment and the problems in integrating disparate access control policies. Section 2 consolidates the work done in past and performs a comparative analysis of various access control models with the proposed framework. Section 3 presents the framework proposed and XACML schema used for designing and verifying the access control policies listed in Appendix A. Section 4 represents the healthcare organizational hierarchies with respect to user and resource attributes. Section 5 deals with verification of the proposed framework using an automated simulator, Access Control Policy Testing (ACPT). The verification is justified through a case study that illustrate the implementation of the framework and its comparison with other approaches. Section 6 concludes and interprets the results obtained that justify the viability of the proposed framework.

2. Literature review

A lot of research has been conducted in past for combining and integrating access control models without exposing the data to illegal and unauthorized disclosure. Each model represent unique features (Karp et al., 2010) that make it different from other models, both, syntactically and semantically. Discretionary Access Control (DAC) model depends on access control lists (ACLs) for determining authorization. In healthcare environment the users experience frequent shift in roles, hence, ACLs need to be optimized (Al-Abdulmohsin, 2009) for quick and secured access to the data. Mandatory Access Control (MAC) model is based on labeling on the resource and the user's credentials. In this environment the variables change once for all and hence cannot respond to dynamically changing environments like healthcare where resource levels change dynamically and require to be in synchronization with the change in user's credentials. Role-based access (RBAC) model (Sandhu et al., 1996; Nyanchama and Osborn, 1999) developed a role-based model using graph theory. It simplifies the security management but challenges the administration of the organizations where several roles are managed for the users simultaneously. The major emphasis is on fine-grain the existing access control policies while designing the secured and interoperable EHR framework.

Various techniques have been deployed to fine-grain access control models with an objective of providing secured and flexible access to the data. Setting up authorization is dependent on the storage mechanism adopted by a particular application. The authorizations may differ in centralized and distributed approach of data storage. Bertino et al. (1994) addresses the semantic data modeling concepts and develops an integrated authorization for interoperable relational and object-oriented databases. Azeez and Venter (2013) propose and simulate RBAC framework that satisfies authorizations and enforces interoperable, scalable and suitable access control for multi-domain grid-based environment. A middleware proposed by Ciampi et al. (2010) evaluates the interoperability facilities in an agent-based architecture where authorizations are