International Journal of Medical Informatics 89 (2016) 25–31

Contents lists available at ScienceDirect

International Journal of Medical Informatics

journal homepage: www.ijmijournal.com

Distributed clinical data sharing via dynamic access-control policy transformation

Fatemeh Rezaeibagha*, Yi Mu

Centre for Computer and Information Security Research, School of Computing and Information Technology, University of Wollongong, NSW, Australia

ARTICLE INFO

Article history:
Received 16 June 2015
Received in revised form 10 February 2016
Accepted 10 February 2016

Keywords:
EHR
Security
Privacy
Data sharing
Access control
Encryption

ABSTRACT

Background: Data sharing in electronic health record (EHR) systems is important for improving the quality of healthcare delivery. Data sharing, however, has raised some security and privacy concerns because healthcare data could be potentially accessible by a variety of users, which could lead to privacy exposure of patients. Without addressing this issue, large-scale adoption and sharing of EHR data are impractical. The traditional solution to the problem is via encryption. Although encryption can be applied to access control, it is not applicable for complex EHR systems that require multiple domains (e.g. public and private clouds) with various access requirements.
Objectives: This study was carried out to address the security and privacy issues of EHR data sharing with our novel access-control mechanism, which captures the scenario of the hybrid clouds and need of access-control policy transformation, to provide secure and privacy-preserving data sharing among different healthcare enterprises.
Methods: We introduce an access-control mechanism with some cryptographic building blocks and present a novel approach for secure EHR data sharing and access-control policy transformation in EHR systems for hybrid clouds.
Results: We propose a useful data sharing system for healthcare providers to handle various EHR users who have various access privileges in different cloud environments. A systematic study has been conducted on data sharing in EHR systems to provide a solution to the security and privacy issues.
Conclusions: In conclusion, we introduce an access-control method for privacy protection of EHRs and EHR policy transformation that allows an EHR access-control policy to be transformed from a private cloud to a public cloud. This method has never been studied previously in the literature. Furthermore, we provide a protocol to demonstrate policy transformation as an application scenario.

1. Introduction

Cloud-based platforms are desirable for delivering electronic health services with ubiquitous network access, scalability, and cost saving [1]. Transferring electronic health records (EHRs) to the cloud poses major threats to privacy, data integrity, and confidentiality. As a result, several regulations and standards such as the HITECH Act, HIPAA, HL7 CDA, CEN 13606, ISO 22600 EHRcom, IHE XDS, and openEHR proposed guidelines and frameworks for sharing and exchanging health information via digital representations of clinical data. However, there are numerous non-standardized communication architectures that have caused semantic divergences. This case reveals that healthcare providers are responsible for protecting their data to ensure that proper access controls are in place [2].

With the growing popularity of cloud computing, EHR data can be stored in the cloud and shared among authorized parties. By using cryptography, secure data sharing can be achieved because encryption can provide a simple form of access control. However, data sharing increases the complexity of key distribution and policy specification of access control. Multi-user settings in the cloud pose challenges to providing an efficient and secure access-control mechanism [3]. Shared data may include patient-sensitive and personal information, such as chronic diseases, mental health issues, psychiatric care, sexual behavior, fertility issues, abortion status, and HIV status, which demand privacy-preserving implementations. Indeed, encryption as a common practice can provide some basic access control against unauthorized access to private EHR data.

Large EHRs are usually handled by distributed computing systems, such as cloud computing systems. Recently, a large number

* Corresponding author.
E-mail address: fr683@uowmail.edu.au (F. Rezaeibagha).

http://dx.doi.org/10.1016/j.ijmedinf.2016.02.002
1386-5056/

of papers about EHR access control with attributed-based encryption (ABE) were published. With ABE, one conveniently manages fine-grained access control in the EHR. This has been seen as a promising approach for cloud-based EHR systems. However, in a practical application, EHR data could be cloud stored in multiple clouds due to the need for scalability and privacy. This aspect of EHR systems has not been investigated.

In this paper, we propose a secure EHR system architecture for secure data sharing, based on several cryptographic building blocks and secret sharing, with role-based access control (RBAC) to protect patients' privacy. To better manage the system, we require data to be stored in different types of clouds, i.e. a public cloud and a private cloud. EHRs stored in the private cloud can only be accessed by the authorized medical professionals, whereas those in the public cloud can be used by medical researchers, pharmaceutical companies, insurance companies, public health agencies, commercial or government agencies, etc. Each cloud requires a RBAC policy that is based on a special type of ABPRE, namely Attribute-Based Proxy Re-encryption. Electronic health record system data sharing is based on the technology of threshold encryption. We consider a practical scenario where an EHR's data can only be accessed while a threshold number of authorized parties are present. It is usually called threshold secret-sharing. This scenario has been outlined in the literature [4].

We provide an approach for policy transformation for transferring private-cloud policies to the public cloud while encrypted data is transferred. This is necessary when private data must be accessed by different parties. Our hierarchical access structure grants access to authorized users and limits access rights to other users in the public domain. To the best of our knowledge, our approach has not been proposed previously.

2. Related work

A large body of literature has investigated the issue of data sharing in cloud computing. We summarize them here.

The work of Wu et al. [5] proposed an access-control mechanism to support selective sharing of composite EHR data from multiple healthcare providers and preserve patient privacy.

In a study that set out to provide patient privacy and accountability in the health information sharing environment, Ahmed et al. [6] suggested *sharing provenance*, which is implementable to the open source CONNECT software to enable eHealth Exchange specifications. Nevertheless, their studies lack the thorough representation of dynamic access-control policy solutions.

In another study, Basu et al. [7] presented *Fusion Architecture*, an experimental cloud-based platform for securely managing and sharing healthcare information at large scale, however, the access structure to clarify data sharing management and the granting of access by different parties were not presented. Mohan et al. [8] proposed MedVault as a patient-centric framework for EHR data sharing in which a source-verifiable health record repository evaluates the requests based on the patient's policy and attributes. Nonetheless, the solution considered neither cloud computing nor policy transformation.

Similarly, Zhang and Liu [9] proposed a security model for sharing and integration of EHR data in the cloud. Encryption and access control were used in the storage server for EHR management with hierarchical and time-bound key management terms. In further studies, [10–13] proposed solutions for privacy-preserving data sharing based on ABE or CP-ABE in the cloud to encrypt data and to provide the hierarchical access structure for fine-grained data sharing. They did not provide policy dynamics as in our proposed scheme.

One of the challenges of data sharing is key management. Yu et al. [14] pointed out data security and access control issues in the EHR sharing within the public domain owing to the heavy computation overhead in key distribution and data management, which occurs in applying fine-grained access control. They used Key-Policy ABE (KP-ABE), Proxy Re-Encryption (PRE), and lazy re-encryption in order to define and enforce access-control policies, but secure and dynamic access rights are demanding.

In the same vein, Wei et al. [15] demonstrated a data-sharing system, in which the data holder encrypts data with the public key and then uploads it to the cloud servers, regardless of various access requirements. Furthermore, Chu et al. [16] proposed a public-key encryption scheme that produces constant-size ciphertexts for efficient delegation of decryption rights in the cloud data sharing in a hierarchical structure. Similarly, in [17], a fine-grained access control and searchable public-key encryption technique were applied in an EHR system. A hierarchical access structure was demonstrated to ensure common trust for information sharing.

Calvillo et al. [18] proposed a service-oriented architecture model focused on security and access control in order to empower patients to manage their own health information. Choe and Yoo [19] presented a "secure multi-agent architecture" that enables healthcare data access to heterogeneous repositories. A local access-control (LAC) system enables the transformation and administration of access policies by using XML, RBAC, and selective encryption. In addition, Chen et al. [20] developed a fine-grained and adaptable access control for healthcare systems through a structured access-control rules in XML. In a further study, Duftschmid et al. [21] undertook an EHR-ARCHE project in order to address the needs to patient's shared EHR during a treatment process through EHR ISO/EN 13606 archetypes into an IHE XDS environment. Although the aforementioned studies aimed at integrating different hospital policies, the possible security exposures and conflicts were not investigated.

3. Proposed architecture

3.1. Data sharing scenario

We are interested in a scenario where patients' data are stored in a private cloud or a public cloud, depending on the access requirements. The data stored in the private cloud can be shared by physicians, but only if a threshold number of authorized parties, e.g. physicians, are present. This feature enabled us to handle the patients' records that are subject to strict privacy control.

This data-sharing application is particularly designed to provide secure interaction among healthcare parties in large geographical areas and scalable systems. We consider an application of large-scale EHR systems in which the treatment process involves concurrent or sequential treatments of different healthcare givers. This application could be used for continuity of care of patients who need regular check-ups and have emergency episodes in chronic conditions. We illustrate a real healthcare scenario as follows.

When a patient visits a general practitioner in a rural clinic to do a diabetes checkup, he might need to visit a central hospital for major blood tests or require rare medicine from a pharmacy. In an acute episode, he visits the Emergency Department to receive initial medical. The ED physician then transfers the patient to the central hospital for major tests and hospitalization. In the treatment process, the clinician in the central hospital, laboratory, pharmacy, and clinics need to share and integrate the patient's health information including treatments, history, test results, primary care visits, and emergency care episodes in the case of sharing experiences resulting in patient treatment. If the patient's data contain sensitive and