

Delegated Authorization Framework for EHR Services using Attribute Based Encryption

Maithilee Joshi

Computer Science and Electrical Engineering
University of Maryland, Baltimore County
Baltimore, MD USA
maithi1@umbc.edu

Karuna Pande Joshi

Information Systems
University of Maryland, Baltimore County
Baltimore, MD, USA
kjoshi@umbc.edu

Tim Finin

Computer Science and Electrical Engineering
University of Maryland, Baltimore County
Baltimore, MD USA
finin@umbc.edu

JIC2 Presentation Abstract at IEEE SERVICES 2021 for IEEE Transactions on Services Computing, doi:10.1109/TSC.2019.2917438

Medical organizations find it challenging to adopt cloud-based Electronic Health Records (EHR) services due to the risk of data breaches and the resulting compromise of patient data. Existing authorization models follow a patient-centric approach for EHR management, where the responsibility of authorizing data access is handled at the patients' end. This creates significant overhead for the patient, who must authorize every access of their health record. It is also not practical given that multiple personnel are typically involved in providing care and that the patient may not always be in a state to provide this authorization.

Hence there is a need to develop a proper authorization delegation mechanism for safe, secure, and easy to use cloud-based EHR Service management. We present a novel, centralized, attribute-based authorization mechanism that integrates Attribute-Based Encryption (ABE) and Semantic Web technologies to allow delegated secure access to patient records. This mechanism transfers the service management overhead from the patient to the medical organization and supports easy delegation of cloud-based EHR's access authority to medical providers.

In ABE, the data is encoded using one set of attributes, and the private key is defined using a different set of attributes. Based on a threshold parameter, the ciphertext can only be deciphered if the two sets of attributes overlap. A user's ciphertext, secret key, and private key are associated with her attrib-

utes. ABE is further divided into Key-Policy Attribute-Based Encryption (KPABE), in which ciphertexts are tagged with attributes corresponding to access control structures, and Ciphertext-Policy Attribute-Based Encryption (CPABE) for implementing ABE using the attributes of the user encrypting the document. Our EHR Manager uses the CPABE toolkit to prototype the research system.

To automate the access policies, we have also developed a complex knowledge graph using RDF and OWL that details the roles and attributes of different medical organization stakeholders and the various relationships between them. In addition, we have used a SWRL-based reasoner to automate access control down to the field level. Our access policy rules are based on the Health Insurance Portability and Accountability Act (HIPAA). We have also developed an open-sourced web-based user interface. Finally, to evaluate the scalability of our system, we performed a performance analysis of the EHR ontology both on the cloud servers and on edge devices.

We currently host this service on the Amazon AWS platform and are developing a version for the OpenStack cloud computing platform. However, many additional security and privacy problems that can be addressed that we leave for future work. For example, more robust authentication mechanisms can help prevent unauthorized access by an attacker who has obtained a physician's credentials, and machine learning can be applied to recognized anomalous patterns of use.