2018 IEEE 11th International Conference on Cloud Computing

Attribute Based Encryption for Secure Access to Cloud Based EHR Systems

Maithilee Joshi, Karuna P. Joshi and Tim Finin
University of Maryland, Baltimore County, Baltimore, MD 21250, USA
Email: {maithi1,karuna.joshi,finin}@umbc.edu

***Abstract*—Medical organizations find it challenging to adopt cloud-based electronic medical records 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 however creates a significant overhead for the patient who has to authorize every access of their health record. This is not practical given the multiple personnel involved in providing care and that at times the patient may not be in a state to provide this authorization. Hence there is a need of developing a proper authorization delegation mechanism for safe, secure and easy cloud-based EHR management. We have developed a novel, centralized, attribute based authorization mechanism that uses Attribute Based Encryption (ABE) and allows for delegated secure access of patient records. This mechanism transfers the service management overhead from the patient to the medical organization and allows easy delegation of cloud-based EHR's access authority to the medical providers. In this paper, we describe this novel ABE approach as well as the prototype system that we have created to illustrate it.**

***Index Terms*—Attribute Based Encryption (ABE), Attribute Based Access Control (ABAC), Electronic Health Record (EHR), Cloud Storage, Semantic Web, Access Broker, Knowledge Graph (Ontology), Cloud Computing**

I. Introduction

An Electronic Health Record (EHR) is an electronic document that details all the relevant clinical reports of a person, over a period of time [1]. In a typical scenario, an EHR records the vital stats, diagnoses, medications, history of immunizations, laboratory and radiology reports, doctor notes etc. Maintaining electronic copies introduces the possibility of attacks on patient data and information privacy [2]. The Health Information Technology for Economic and Clinical Health (HITECH) Act [3] promotes a meaningful use of electronic versions of patient health records. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) [4], [5] regulates the management and distribution of medical records by establishing standards for preserving the security and privacy of medical health data. Developing an EHR management solution that complies with all the legal and ethical standards becomes a huge research and development challenge.

The recent past has seen an increased adoption of cloud-based EHR services [6], [7]. This can be attributed to the fact that cloud computing guarantees a high level of availability and elasticity along with the advantage of major cost cutting. Currently, there exist a number of cloud-based EHR services like, CureMD [www.curemd.com], Practice Fusion [www.practicefusion.com], Athenahealth [www.athenahealth.com] etc. Organizations like GE Healthcare [www.gehealthcare.com] and Epic Health Services [www.epichealthservices.com] are also investing in cloud-based EHR services. Various research efforts have been proposed with major focus on secure, cloud-based EHR systems [6], [7]. However, majority of the proposed approaches lack in guaranteeing a attribute-based access control and encryption mechanism.

In this paper, we describe the cloud-based EHR management solution that we developed to guarantee a secure, encrypted access control and patient data security mechanism, down to the field level. Our system can be used by medical organizations for securely maintaining EHRs, at a very low operational cost. It incorporates a semantically rich, policy based approach using Attribute Based Access Control (ABAC) [8] to comprehensively evaluate a person's access to the system. Further, to guarantee a tight data security, we use Attribute Based Encryption (ABE) [9] at a field-level to encrypt and store the patient EHRs.

We have used Semantic Web technologies to implement this system. We have developed a HIPAA compliant knowledge graph (ontology) by referencing the HIPAA Ontology [10] previously developed by us. This knowledge graph details the roles and attributes of the different stakeholders of the medical organization along with the various relationships between them, and is stored at the EHR cloud service provider location. To implement secure access control and attribute based encryption, our system extracts the user and EHR field attributes from this knowledge graph. Apart from this, our approach records every patient visit as a separate node in the knowledge graph. This facilitates easy querying and faster data access operations.

The rest of the paper is organized as follows – We discuss related work in Section II, our system architecture in Section III and our system implementation in Section IV. We present our conclusions and future work in Section V.

II. Related Work

Automating the medical health record management system has received a lot of research focus [11], [12], [13], [14]. The privacy and security of the patient health record being of utmost importance, this field of research has seen various approaches being suggested [12], [13], [15]. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

2159-6190/18/$31.00 ©2018 IEEE
DOI 10.1109/CLOUD.2018.00139

provides data privacy, security and safeguarding acts for protecting electronic medical information of individuals [4], [5]. The Health Information Technology for Economic and Clinical Health (HITECH) Act aims towards maintaining electronic medical records by ensuring quality, safety, efficiency, privacy and security [3].

In our previous work, we developed a semantically rich access control model based on Attribute Based Access Control (ABAC) [16]. This model evaluated an access decision based on the attributes of the user and those of the document. This work demonstrated the use of policy-based, semantic web approach of implementing ABAC at a document level. In this paper, we have improved this system to evaluate an access decision on the fields of a document. Along with this, we have improved the system to categorize the permitted access instead of just a binary decision.

Various access control models have been proposed namely Mandatory Access Control (MAC), Role Based Access Control (RBAC) [17], etc. Jin et. al. proposed a model called as the Attribute Based Access Control (ABAC) [8]. Modeling access control policies has been a topic of interest. XACML is a policy model, based on the XML specification language [18] which uses attributes to impose access control.

For representing policies and rules formally, The Web Ontology Language (OWL) [19], [20], [21] serves to be very efficient while representing security policies. OWL representation of ABAC policies have been presented in [21].

To protect data privacy and threats, various encryption models have been proposed. Attribute Based Encryption (ABE) is one such interesting approach where the ciphertext, the secret key and the private key of the user are associated with the user's attributes [9], [22], [23]. Bethencourt et. al. have developed a system called the Ciphertext-Policy Attribute Based Encryption (CPABE) for implementing ABE using the attributes of the user encrypting the document [22]. In our system, we use the CPABE toolkit to prototype our research effort.

Attribute based encryption has been one of chosen technologies for electronic health record management systems too [24], [25], [26]. Akinyele et. al. at the John Hopkins University and the John Hopkins Medical Institutions have presented a design and implementation of Electronic Medical Records (EMRs) using attribute based encryption on mobile devices [24]. However, their model does not support a field level encryption of the EHR. Researchers at Microsoft developed a patient controlled electronic medical record system with attribute based encryption [25]. This system put all the access control in the patient's hands. This introduces a lot of control overhead involved on the patient's end. In our system however, we do not impose any overhead on the patient. The central system handles all the secure access and distribution of the EHR.

III. System Architecture

As shown in Figure 1, users of the medical organization like doctors, nurses, pharmacists, etc. request login to the system to which the system carries out a comprehensive access control check to authenticate the users using the *Access Broker Unit*. In our previous work [16], we have developed this unit which uses Attribute Based Access Control (ABAC) to semantically carry out a strong access control mechanism. In this paper we have modified the *Access Broker* to further categorize the access decision instead of just a boolean decision.

Once the user modifies a field, the system then encrypts the updated details of the accessed EHR fields by employing the *Attribute Based Encryption (ABE) Unit*. This unit extracts the user's attributes from the main ontology which is stored with a public cloud service provider, in our case Amazon Web Services (AWS) [aws.amazon.com]. Encryption keys are provided by the *Key Generation Unit*. The encrypted text then needs to be updated in the EHR Ontology. To do this, a new node is created which records all the details of a patient's visit to the medical organization. Finally, this ontology is saved with a cloud service provider. Following is a mathematical representation of the system implementation.

User set U = $\{U_1, U_2, ...U_n\}$
User Attribute Set US = $\{UA_1, UA_2, UA_3, ...UA_n\}$
EHR set E = $\{E_1, E_2, ...E_n\}$
EHR attribute set ES = $\{EA_1, EA_2, EA_3, ...EA_n\}$
EHR Fields Set EF = $\{EF_1, EF_2, ...EF_n\}$
EHR Fields Subset EFS $\subset$ *EF*
Policy set PS = $\{PS_1, PS_2, ...PS_n\}$
Decryption Policy set DS = $\{DS_1, DS_2, ...DS_n\}$
$\forall$ *User U,* $\exists$ *User Attribute Set US*

For evaluating access decision
For each User X $\wedge$ *EHR Y* $\wedge$ *EHR Fields Set Z,*
If US satisfies any one from policy from PS $\rightarrow$ *Read_and_or_Write (User X , EHR Y, EFS)*

For encryption using ABE
For each User X $\wedge$ *EHR Y,* $\exists$ *Fields Subset Z,*
X $\wedge$ *Y* $\wedge$ *User Attribute Set US* $\wedge$ *Z* $\rightarrow$ *Encrypted EHR field where US* $\subset$ *DS*

For decryption using ABE
If User Attribute Set US $\subset$ *DS*
US $\wedge$ *EF* $\rightarrow$ *Decrypted EFS*

Following sections describe each sub-module in detail.

A. Access Broker

The primary concept behind this module is the Attribute Based Access Control (ABAC). The *Access Broker* consists of 3 main sub-modules - the *Organizational Knowledge Base*, the *Rule Based Engine* and the *Policy Unit*.

The *Organizational Knowledge Base* stores all the details, of every entity belonging to the medical organization, in the form of an ontology - the *EHR Ontology*. The *Policy Unit* stores all the access policies in terms of a organizational confidentiality policy. The *Rule Based Engine* uses the Semantic Web Rule Language (SWRL) to use the confidentiality policies for implementing access control decisions. The *Rule Based Engine* requires user and document attributes from the ontology for carrying out access control decisions [16]. The following figure shows an example SWRL rule where, a *Junior*

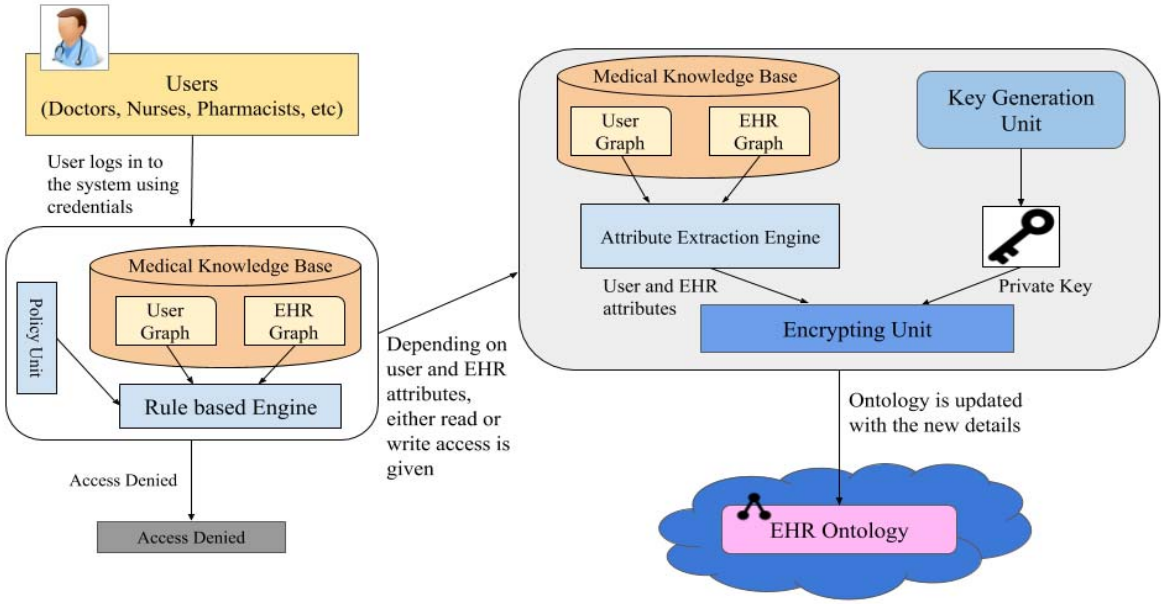

Fig. 1: System Architecture

Doctor with certain attributes, can access only those fields, to which a *Senior Doctor* to whom this *Junior Doctor* reports to, has access to.

```
JuniorDoctor(?jd) ^ HospitalWard(?hw) ^
    SeniorDoctor(?sd) ^ Certification(?c) ^
    EHR(Medication) ^ EHR(Diagnoses) ^
    EHR(Allergies) ^ worksIn(?sd, ?hw) ^
    worksIn(?jd, ?hw) ^ isCertifiedBy(?jd,
    ?c) ^ reportsTo(?jd, ?sd) ^
    canModifyMedication(?sd, true) ^
    canModifyAllergies(?sd, true) ^
    canModifyDiagnoses(?sd, true) ->
    canReadMedication(?jd, true) ^
    canReadDiagnoses(?jd, true) ^
    canModifyAllergies(?jd, true)
```

B. Attribute-based Encryption Unit

This module works on the principles of Attribute Based Encryption (ABE)[22]. Here, the user attributes serve as encryption/decryption keys for document protection. The *ABE unit* consists of 3 sub-modules - the *Organizational Knowledge Base*, the *Attribute Extraction Unit* and lastly the *Encryption unit*. The *Attribute Extraction Unit* queries the EHR Ontology to retrieve the user and the EHR field attributes. We have used the CipherText-Policy Attribute Based Encryption (CPABE) [acsc.cs.utexas.edu/cpabe] [23] for encryption purposes. The *Encrypting Unit* now encrypts the modified EHR field. To update the *EHR Ontology* with the modified EHR field, it creates a new node in the *EHR Ontology*. The Key Generation Unit generates the keys required for ABE and provides it to the *ABE unit*.

C. EHR Ontology

The *EHR Ontology* is a HIPAA complaint ontology [10] which stores all the user and EHR attributes represented as a knowledge graph. This ontology details the roles and attributes of the different stakeholders of the medical organization along with the various relationships between them.

D. Cloud Service Provider

The cloud service provider is a public cloud platform. The encrypted data is migrated to the cloud service provider which hosts the *EHR Ontology*.

IV. System Implementation

The EHR Manager Application is an open-source web application developed in Python to manage the field-level, attribute based encryption and access control of patient EHRs.

The EHR Manager Application is built on the principles of the Model-View-Controller (MVC) architecture. Python Django is an open-source web based framework which supports clean and faster web development. To design and develop the *EHR Ontology*, developed by the Stanford Center for Biomedical Informatics Research, we used the tool Protege[protege.stanford.edu], an open-source, free, knowledge graph editor and management system. The Semantic Web Rule Language (SWRL) is used in querying and manipulating the knowledge graph. To extract the user and EHR field attributes out of the ontology, an open-source library called *rdflib* is used which queries the ontology and extracts the necessary user and EHR field attributes. The CipherText-Policy Attribute Based Encryption (CPABE) library is used for carrying out the

encryption [23]. The CPABE library provides four command-line tools - *cpabe-setup, cpabe-keygen, cpabe-enc* and *cpabe-dec*. In this way, the EHR Manager harnesses the semantic web and attribute based technologies to successfully guarantee a strong, robust, EHR managing application at a field-level.

A. Proof of Concept

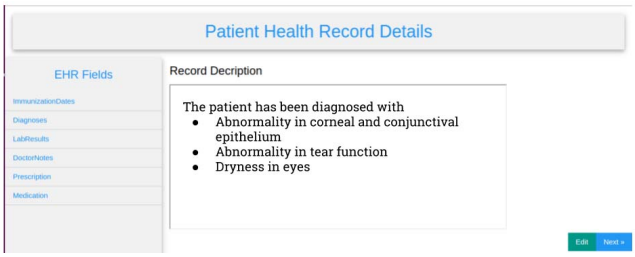

Fig. 2: Scenario 1: Full access

As mentioned above, the EHR Manager application allows healthcare providers to treat their patients. This system uses attribute based access control for controlling access to patient data and attribute based encryption for storing the data securely. Following figures show two scenarios- the first one is where a doctor with various attributes gets access to all the fields of an EHR, whereas another nurse gets access to only a subset of the fields because of the difference in attributes. To evaluate our system, we conducted a user study where we

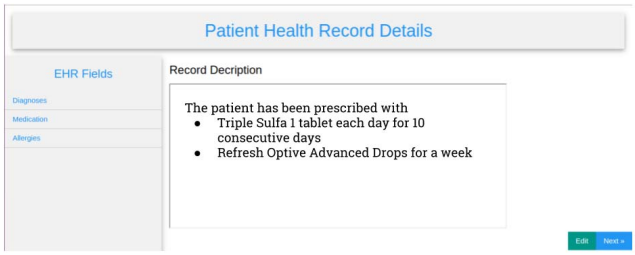

Fig. 3: Scenario 2: Limited access

asked a few domain experts to use our system application. The users were briefed about the usage of organization specific confidentiality policies for accessing the EHRs. The users were asked to enter patient details that could cover all different scenarios where they thought the system could fail. All the users could easily perform the task with some minor help from one of the authors.

V. Conclusion

In this paper we developed an attribute based, field level, document encryption for managing the access and data security of cloud-based EHRs. In our approach we designed and developed a complex knowledge graph that details the roles and attributes of different stakeholders of the medical organization along with the various relationships between them. We also developed an open-source, easy to use user interface.

In future, we plan to solve the inference problem commonly seen in semantic web solutions by building a double layer of attribute based encryption.

Acknowledgment

This research was supported by the Office of Naval Research under grants N00014-15-1-2228 and N00014-16-WX-01489. We thank Dr. Seung Geol Choi (USNA), Dr. Eliot Siegel (University of Maryland Medical Center) and members of the Ebiquity Research Group for their vital feedback.

References

[1] K. Häyrinen, K. Saranto, and P. Nykänen, "Definition, structure, content, use and impacts of electronic health records: a review of the research literature,"
[2] R. C. Barrows Jr and P. D. Clayton, "Privacy, confidentiality, and electronic medical records,"
[3] D. Blumenthal, "Launching hitech,"
[4] C. for Disease Control, Prevention, *et al.*, "Hipaa privacy rule and public health. guidance from cdc and the us department of health and human services,"
[5] U. D. of Health, H. Services, *et al.*, "Summary of the hipaa privacy rule,"
[6] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,"
[7] A. Bahga and V. K. Madisetti, "A cloud-based approach for interoperable electronic health records (ehrs),"
[8] X. Jin, R. Krishnan, and R. Sandhu, "A unified attribute-based access control model covering dac, mac and rbac,"
[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data,"
[10] K. P. Joshi, Y. Yesha, and T. Finin, "An ontology for a hipaa compliant cloud service," in *4th International IBM Cloud Academy Conference ICACON 2016*.
[11] J. A. Evans, "Electronic medical records system."
[12] E. H. Shortliffe *et al.*, "The evolution of electronic medical records,"
[13] M. Lavin and M. Nathan, "System and method for managing patient medical records."
[14] S. Narayan, M. Gagné, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," in *CCSW*.
[15] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*.
[16] M. Joshi, S. Mittal, K. P. Joshi, and T. Finin, "Semantically rich, oblivious access control using abac for secure cloud storage,"
[17] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models,"
[18] A. Anderson, A. Nadalin, B. Parducci, D. Engovatov, H. Lockhart, M. Kudo, P. Humenn, S. Godik, S. Anderson, S. Crocker, *et al.*, "extensible access control markup language (xacml) version 1.0,"
[19] D. L. McGuinness, F. Van Harmelen, *et al.*, "Owl web ontology language overview," *W3C recommendation*.
[20] L. Kagal, T. Finin, and A. Joshi, "A policy language for a pervasive computing environment,"
[21] N. K. Sharma and A. Joshi, "Representing attribute based access control policies in owl," in *Semantic Computing (ICSC), 2016 IEEE Tenth International Conference on*.
[22] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption,"
[23] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *International Workshop on Public Key Cryptography*.
[24] J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. Peterson, and A. D. Rubin, "Securing electronic medical records using attribute-based encryption on mobile devices,"
[25] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records,"
[26] S. Narayan, M. Gagné, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure,"