2019 IEEE International Conference on Edge Computing (EDGE)

Multi Authority Access Control in a Cloud EHR System with MA-ABE

Sharad Dixit
Department of CSEE
University of Maryland, Baltimore County
Email: sdixit1@umbc.edu

Karuna P. Joshi
Department of Information Systems
University of Maryland, Baltimore County
Email: kjoshi1@umbc.edu

Seung Geol Choi
Department of Computer Science
United States Naval Academy
Email: choi@usna.edu

***Abstract*—With the rapid adoption of Cloud-based Electronic Health Record (EHR) systems, health providers are particularly concerned about managing data privacy on the cloud. Existing approaches have either a scalability bottleneck by requiring that patients approve each sharing of their medical data or a trust bottleneck by having a single authority control every access thereby creating the problem of a single point of attack.**

To address both these bottlenecks, we have developed a novel framework that enables policy based multi-authority access authorization to EHR systems accessed by multiple care providers from different locations or organizations. This framework, which resides on the Edge, has been built using the Multi-Authority Attribute Based Encryption (MA-ABE) and Semantic Web technologies to provide a secure, semantically rich approach to facilitate secure data sharing among organizations who manage different attributes of end users using a shared dataset. In this paper, we describe our novel approach along with the proof of concept prototype that we created to evaluate our framework.

***Index Terms*—Multi-Authority Attribute Based Encryption (MA-ABE); Attribute Based Access Control (ABAC); Knowledge Graph (Ontologies); Cloud Computing; Access Handler; Document Processor & Crypto Module**

I. Introduction

Medical organizations have increasingly started to adopt cloud-based Electronic Health Record (EHR) systems [1], [2], [3], [4] to avail the significant cost reduction as well as the flexibility and high availability provided by these systems. These cloud-based EHR systems allow an organization to take advantage of the efficiency and scalability features of cloud storage that enable fast retrieval and sharing of medical data. However, storing electronic copies remotely with third-party cloud servers increases the possibility of attacks and data breaches leading to privacy concerns [5], which has impeded wide adoption of such services.

Existing approaches for EHR data privacy. In order to enforce privacy of medical data, researchers have considered an approach of patient-centric privacy [6], [7], [8], where the patient is responsible for authorizing every access decision. Although ideal from a privacy standpoint, involving a patient with every access decision creates a significant system overhead, causing considerable damage to the scalability of the system.

Due to the aforementioned issues, most of the research works consider a central authority (CA) to manage an access control mechanism with encryption [8], [9], [10], [11]. However, this framework creates a load bottleneck on CA. If CA becomes unavailable, due to either a denial of service attack or a software/hardware error, it would stop the entire system from working. More importantly, the system puts too much trust on CA. if CA stops being trustworthy, data privacy of the entire system would be endangered.

Our Work. To overcome the shortcomings of previous works, we propose a novel EHR access framework that guarantees a secure *encrypted* access control mechanism in a *multi-authority* environment. In situations where caregivers can belong to different organizations and be working in different context (location, time etc.), data access policies are often dictated by Multiple Authorities (MA). Our framework enables MA to specify different set of attributes for a caregiver and allows access to patient EHR only if all attribute conditions are satisfied.

Our framework's architecture is based on the principles of Edge Computing [12], where we have established the "edge" as a strong boundary for communication outside the organization. In particular, we have implemented a secure access control mechanism for user authentication and a robust crypto module for data encryption in order to tighten security and privacy before moving the data out of the organization. Our framework furnishes rich semantics by implementing secure access control mechanism based on the principles of Attribute-Based Access Control (ABAC) [13], [14] in a multi-authority environment, providing semantically rich policy-based access decisions. We have utilized Multi-Authority Attribute-Based Encryption (MA-ABE) scheme [15] for data encryption to more strengthen our framework.

Related Work. Various access control mechanisms such as the fixed access control list (ACL), Mandatory Access Control (MAC), Role Based Access Control (RBAC) etc. have been applied for securing documents. However, these models are not sufficient for an organization with a complex organizational structure. In our scheme, we have utilized Attribute Based Access Control (ABAC) which is an enhancement over all the models where a number of user's multi-valued attributes are evaluated against the access policy before providing an access decision.

978-1-7281-2708-8/19/$31.00 ©2019 IEEE
DOI 10.1109/EDGE.2019.00032

To obtain privacy and security of medical records, an increasing interest is seen in applying Attribute Based Encryption (ABE) to develop secure systems for Electronic Health Record (EHR). In particular, Narayan et al. [9] proposed an expressive fine-grained encrypted EHR system where a patient's EHR file was encrypted using the broadcast variant of CP-ABE (ciphertext policy ABE) that allowed users and attributes revocation. Akinyele et al. [11] integrated ABE in his proposed infrastructure to secure electronic medical records on mobile devices or cloud servers. Recently, Joshi et al. [16] proposed a secure encrypted access control application which implemented CP-ABE [17] for storing encrypted electronic health records with Amazon cloud service provider.

However, the above ABE-based systems have a shortcoming that they assume a single central authority in the system. All the trust and workload of issuing keys and attribute related tasks like verifying ingenuity of user attributes is handled by this central authority which not only creates a load bottleneck but also creates privacy and security issues as it gives the central authority the power to access all the encrypted documents. Moreover, most of the works above do not provide a semantically rich access control mechanism for fine-grained access to the system.

II. System Framework

In our EHR system, there are multiple users, authorities and data owners, but a single cloud service provider stores all the EHR documents in the cloud storage. Users come from a broad medical universe; each user receives access right based on his attributes matched against the confidential policies defined by the organizations. Data owners are patients, and they have complete read access to their EHR documents. The cloud service provider may be compromised by an adversary as well. In this case, we assume that a corrupted cloud service provider will behave in an honest-but-curious manner [18]. Our framework is divided into two major parts, where we have defined our secure "edge" as the organizational boundary with entities inside boundary considered as trusted units whereas outside as untrusted (see Figure 1 for the overall system architecture).

Access Handler module. Different users request a login to the system to which the initial authentication is performed by traditional challenge-response protocols. If the user qualifies the initial authentication phase, then a comprehensive access control decision is evaluated in the terminal authentication phase where read, write or no access is provided to users using Attribute Based Access Control (ABAC) to semantically carry out strong access control mechanism. To evaluate the extensive access decision, respective semantics of the user and document (attributes instances) are extracted from the organizational knowledge base which stores all the details of every establishment in the EHR domain in the form of an ontology - *Multi-Authority EHR Ontology*. Conclusively, *Rule Based Engine* carries out an access decision by matching the extracted attribute instances against the confidential access policies defined by an organization stored within the *Policy unit* in the form of Semantic Web Rule Language (SWRL) rules.

Document Processor & Crypto module. If the access handler permits the request, then the request is forwarded to the *Document Processor & Crypto Module*. We have implemented Multi-Authority Attribute Based Encryption (MA-ABE) [15] with Symmetric Encryption for encryption purpose in this module by using Charm-Framework [19] to develop a complete cryptographically secure encryption toolkit for our framework. If decision was read, then the *Document Processor Module* fetches the document from the cloud server and waits for the decryption keys to be provided by the user, which the user obtains from his respective bounded multiple controlling authorities in the system. If the decryption keys provided by the user are valid then the *Decryption Unit* and *Key Generation Unit* of the *Crypto Module* decrypts the EHR document. In the case of write access, all modules function as in the case of reading. However, after the user modifies the document, the *Encryption Unit* of the *Crypto Module* encrypts the file using the encryption keys provided by *Key Generation Unit* in accordance with the access policy provided by the organization. The encrypted document is then stored on the cloud server while creating a new node recording all the details of the modifications in the patients EHR.

Multi-Authority EHR Ontology & Cloud Service Provider. The Cloud Service Provider provides an environment outside the organizational boundary where we host our Multi-Authority EHR ontology which holds all the details of the different authorities, users, and documents as instances of classes developed in the ontology related to the medical domain, while complying to HIPAA privacy and security rules [20]. The encrypted EHR data is stored on the cloud platform as nodes of the ontology.

III. Implementation and Evaluation

Implementation. Initially, in our framework global public parameters are generated by *Crypto Module*. Based on the global public parameters, each authority in the system generates their respective public and master secret key pairs. Then, each authority provides users with their secret keys associated with their respective attributes. An EHR document in our system is assumed to be as a directory of encrypted files stored in sub-folders with the access policy stored with it. We have used Protege [protege.stanford.edu], which is an open-source, free, knowledge graph editor and management system, when we develop our Multi-Authority EHR ontology. For querying, we use *SPARQL* with *Apache Jena* library to extract authority, user and document attributes, and relationship between them. Semantic Web Rule Language (SWRL) rules are used to manipulate and obtain inference from the ontology.

Evaluation. For evaluation of our system, we developed a proof of concept prototype that is described below. Suppose an EHR of a patient Bob is enforced and encrypted by our

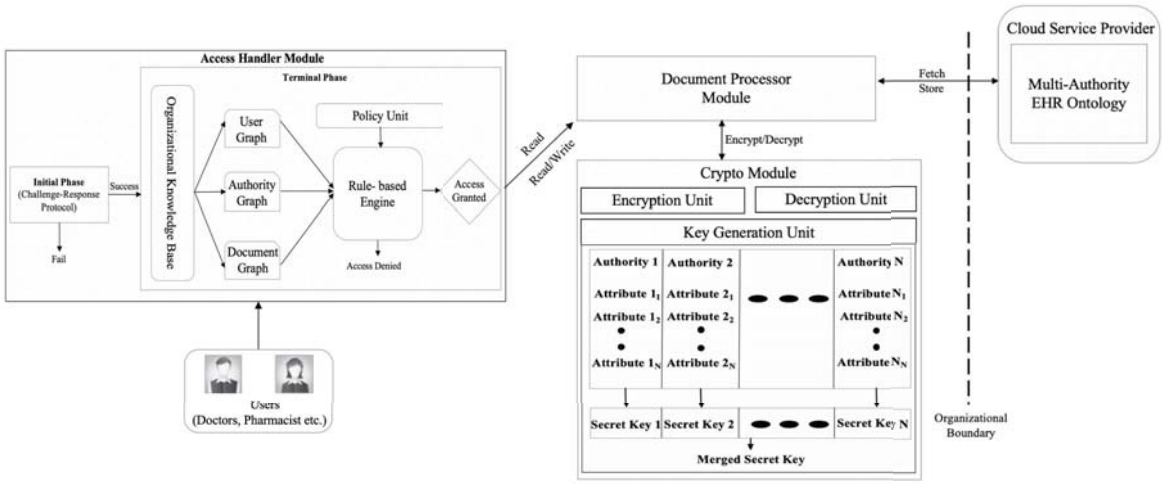

Fig. 1: Overall System Architecture

Fig. 2: Prototype User Interface

framework under the an organization's access policy. If any user is able to qualify the access policy then read access decision is provided by Access Handler module. Suppose Alice is an authorized user and her attributes match against Bob's EHR access policy, then after singing into our system, a "read" access decision is provided by *Access Handler Module* of our framework. Figure 2 depicts the prototype user interface of our system for a user Alice after signing into our system. Access decisions are provided by matching the access policies against attributes of the user.

To decrypt the file, Alice obtains secret keys associated with her attributes from her respective authorities. If all the secret keys provided by the user to our system are certified and valid then our *Crypto Module* performs decryption, allowing the user to only have read access.

Acknowledgements. This work has been supported by Office of Naval Research under grants N00014-18-1-2453 and N00014-19-WX-00568.

REFERENCES

[1] A. Bahga and V. K. Madisetti, "A cloud-based approach for interoperable electronic health records (ehrs)," *IEEE Journal of Biomedical and Health Informatics*, vol. 17, pp. 894–906, 2013.

[2] 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," *IEEE Transactions on Parallel and Distributed Systems*.

[3] H. Lhr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud," 01 2010, pp. 220–229.

[4] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted data in cloud computing," in *2011 31st International Conference on Distributed Computing Systems*, June 2011, pp. 383–392.

[5] J. Barrows, Randolph C. and P. D. Clayton, "Privacy, Confidentiality, and Electronic Medical Records," *Journal of the American Medical Informatics Association*, vol. 3, no. 2, pp. 139–148, 03 1996.

[6] K. D. Mandl, P. Szolovits, and I. S. Kohane, "Public standards and patients' control: how to keep electronic medical records accessible but private," *BMJ*, vol. 322, pp. 283–7, Feb 3 2001.

[7] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: Ensuring privacy of electronic medical records," 2009.

[8] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *2010 Proceedings IEEE INFOCOM*, March 2010, pp. 1–9.

[9] S. Narayan, M. Gagn, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," 01 2010, pp. 47–52.

[10] L. Ibraimi, M. Asim, and M. Petkovi, "Secure management of personal health records by applying attribute-based encryption."

[11] J. A. Akinyele, C. U. Lehmann, M. D. Green, M. W. Pagano, Z. N. Peterson, and A. D. Rubin, "Self-protecting electronic medical records using attribute-based encryption," 2010.

[12] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, Oct 2016.

[13] N. K. Sharma and A. Joshi, "Representing attribute based access control policies in owl," in *ICSC*, Feb 2016, pp. 333–336.

[14] X. Jin, R. Krishnan, and R. Sandhu, "A unified attribute-based access control model covering dac, mac and rbac," N. Cuppens-Boulahia, F. Cuppens, and J. Garcia-Alfaro, Eds.

[15] Y. Rouselakis and B. Waters, "Efficient statically-secure large-universe multi-authority attribute-based encryption," in *Financial Cryptography and Data Security*, 2015, pp. 315–332.

[16] M. Joshi, K. Joshi, and T. Finin, "Attribute based encryption for secure access to cloud based ehr systems," 07 2018, pp. 932–935.

[17] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *ACM CCS*.

[18] T. Mather, S. Kumaraswamy, and S. Latif, "Cloud security and privacy: An enterprise perspective on risks andcompliance," 01 2009.

[19] J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, "Charm: a framework for rapidly prototyping cryptosystems," *Journal of Cryptographic Engineering*.

[20] Y. Y. Karuna Pande Joshi and T. Finin, "An ontology for a hipaa compliant cloud service," in *4th International IBM Cloud Academy Conference ICACON 2016*. IBM, June 2016.