International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 07 | July 2020 www.irjet.net p-ISSN: 2395-0072

Secure Electronic Health Record Storage System Using Attribute Based Encryption Technique

Ms. Farog Fatema Khan[1], Dr. G.R. Bamnote[2]

[1]Department of Computer Science and Engineering, PRMITR, Badnera, Maharshtra, India
[2]HOD of Computer Science and Engineering, PRMITR, Badnera, Maharashtra, India

---

Abstract: *There are many medical organizations who 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. Privacy of patient and the security of their information is the most imperative barrier to entry when considering the adoption of electronic health records in healthcare industry. And therefore, there is a need to develop a proper mechanism for safe, secure and easy to use cloud-based EHR Service management. For addressing these problems, a secure cloud based electronic health record storage system is proposed here, in which patient's data will be maintained on cloud server securely using Attribute Based Encryption (ABE) technique. To improve existing ABE technique, a new attribute-based encryption technique with unique attribute id is used. Along with it to improve the security of the document, a Hybrid Encryption algorithm is proposed.*

Keywords: Electronic Health Records (EHR), Attribute Based Encryption (ABE), Hybrid Encryption

1. INTRODUCTION

Due to the advancement of technology specially in medical sciences it has turned healthcare organizations into customer-oriented environments. These organizations are in a quest for quality improvement. This will not be achieved without anytime access to high quality information [1].

International Organization for Standardization (ISO) describe that Electronic Health Record (EHR) is a storage, secure exchange and access to patient information in digital format by several authorized users. This information includes the patient's past, present, and future information. Objective of EHR is to support the maintenance of integrated, efficient and quality health [2]. Electronic Health Record (EHR) can be defined as an electronic version of a patient's health history that documents all the relevant clinical details over a period of time [3] and is maintained by healthcare providers. These EHRs help organizations provide improved healthcare services by automating patient information access and management.

In developing of EHR, some of the barriers are encountered, which can be categorized as technical, organizational, personal, financial, and moral-legal barriers [4]. Hence in regard to this, the use of new technologies such as cloud computing is effective in its successful implementation. Cloud computing is the computation that was done by a group of remote servers that form a network. It leads to centralized storage of data and online access to services and computer resources; simply cloud computing is the acquisition to computing resources through the Internet [5],[6].

There are many security and privacy issues that have raised difficulties for the adoption of cloud-based EHR systems. In the United States, compliance to HIPAA (Health Insurance Portability and Accountability Act) [7] is often cited as the requirement to preserve the confidentiality of medical records including EHRs. As cloud service providers are not trusted to store EHRs unencrypted, even when access controls are in place [8], EHR encryption must be required in cloud-based EHR systems.

2. RELATED WORK

This section gives a brief introduction into the related work done on this subject:

2.1 Attribute Based Access Control Work

In their work, Joshi et.al. developed a semantically rich access control model based on Attribute Based Access Control (ABAC) [9]. The model evaluated an access decision based on the attributes of the user requesting a document and those of the requested document. Then access control decisions were evaluated against an organizational confidentiality policy. Their work demonstrated the use of policy-based, semantic web approach of implementing ABAC at a document level. Apart from this, the previously developed system demonstrated the concept of edge computing [10] where the organizational boundary was considered to be the edge of the system. The cloud service provider was considered as an untrusted entity and thus laid beneath the organizational edge.

2.2 Attribute Based Encryption

Various encryption models have been proposed to protect data privacy and threats. Attribute Based Encryption (ABE)

is one approach where a user's ciphertext, secret key and private key are associated with her attributes [11]. In their paper Goyal et. al. proposed an attribute-based system called the Key-Policy Attribute Based Encryption (KPABE) [11] in which ciphertexts are tagged with attributes corresponding to access control structures. Their model supports Hierarchical Identity-Based Encryption (HIBE). Also, 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 [12]. The EHR Manager uses the CPABE toolkit to prototype the research effort. ABE has been one of chosen technologies for electronic health record management systems too [13], [14].

3. SECURE EHR STORAGE SYSTEM

Our primary objective is to develop a highly secure, attribute-based access mechanism for a Cloud based EHR service that will provide flexibility of data access to end users along with a sophisticated data encryption scheme. So here a secure cloud based electronic health record storage system is proposed, in which patient's data will be maintained on cloud server securely using ABE technique. To improve existing ABE technique a new attribute-based encryption technique with unique attribute id is proposed. In this technique one unique attribute id is allotted to each document and using that unique attribute id, the access attributes for that document will be maintained on separate server rather than cloud server.

The process in the system begins by concentrating on implementing a policy defined attribute-based access control component of the EHR system and hence designed a simple user-id/password-based authentication scheme. Then the medical organization user's first login to the system using their credentials and the system carries out an access control check to authenticate the user and requested actions are evaluated with respect to access rules, user attributes and EHR attributes. If the action is permitted, any required updates to the EHR are made.

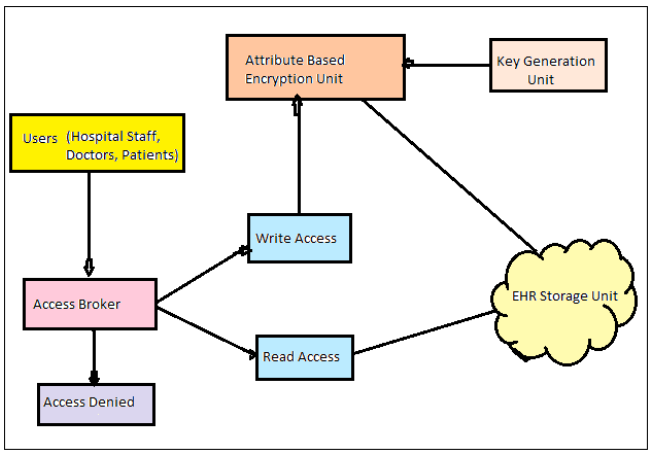

Figure 1: System Architecture

The system next waits for the user to access the EHR. Once done, it then needs to encrypt the updated details of the accessed EHR fields, which is done by the Encryption Unit. This unit uses modified Attribute Based Encryption for encrypting the EHR field. It extracts the user's attributes from the main ontology which is stored in attributes storage server which is the separate server rather than the cloud server. The key generation is done by the Key Generation Unit, which uses the keys provided by the Encryption Unit to encrypt the EHR. The encrypted text is then uploaded to the cloud where hybrid encryption will be used.

In this electronic health record storage system, the patient's data will be maintained on cloud server securely using ABE technique. To improve existing ABE technique, new attribute-based encryption technique with unique attribute id is proposed. In this technique one unique attribute id is allotted to each document and using that unique attribute id, the access attributes for that document will be maintained on separate server rather than cloud server. As we are using attribute ID to encrypt the documents using ABE instead of complete attributes, there is no need to update the cipher text of documents. We have to update the Attribute storage database only. It will reduce the time required for decryption and re-encryption in case if patient changes/ add access permission.

Along with it to improve the security of the document a Hybrid Encryption algorithm is proposed. In hybrid encryption algorithm, we proposed a combination of AES and RC6 algorithm. In hybrid encryption, document will be converted into four parts. AES and RC6 algorithms will be applied on alternate parts with separate keys.

3.1. Algorithm steps

Step 1- Upload document/image file.
Step 2- Read bytes of uploaded document.
Step 3- Set bytes[] = ReadBytes(Doc)
Step 4- Split bytes[] into 4 parts
Step 5- Set len = bytes[].len/4
Step 6- Set b1[] = RangeBytes(bytes[], cnt, len)
Cnt = cnt+len
Step 7- Set b2[] = RangeBytes(bytes[], cnt, len)
Cnt = cnt+len
Step 8- Set b3[] = RangeBytes(bytes[], cnt, len)
Step 9- if len%2 == 0 then
Set lastpartLen = len
Else
Set lastpartLen = len+1
End if
Step 10- Set b4[]= RangeBytes(bytes[], cnt, len)
Step 11- Set AK (Attribute key) = Unique attribute key for document
Step 12- Set k1 = (Generate 32 byte key with Attribute key Ak for AES)

Set k2 = (Generate 32 byte key with Attribute key Ak for RC6)

Step 13- Encrypt b1[] using AES and key k1
Encrypt b2[] using RC6 and key k2
Encrypt b3[] using AES and key k1
Encrypt b4[] using RC6 and key k2

Step 14- Combine all encrypted parts to get encrypted file.

Step 15- Store encrypted file on cloud server.

Proposed system introduces attribute key generation specific to medical report i.e. document getting uploaded and not to user. The same attribute key is associated to each user who is given the permission to access medical report. So whenever new permission is allotted, revoked or updated only the permission details to corresponding user are updated in database and not the attribute key. Also, when generating the secrete key for physical encryption of the document the same attribute key is used.

4. EXPERIMENTAL RESULTS

We considered certain reports of the patients which were uploaded in the application. And the access permission is given by the patients to different users. Now calculated the time required by the existing system and proposed system.

File Id	File Title	File Size (Bytes)	No of Permissions	Proposed Time (µs)	Existing Time (µs)
121	Blood Report	24860	3	228	686
122	Sugar Report	24860	1	189	189
123	XRay Scans	132139	2	245	491
124	Test Report	666961	2	208	417
125	Citiscan Report	24860	3	182	547

Table 1: Time Evalution

As we can see from the graphs below, proposed system requires lesser time for attribute key generation as it is not user specific. While in existing system the attribute generation is more time consuming as it is to be updated on each permission transaction.

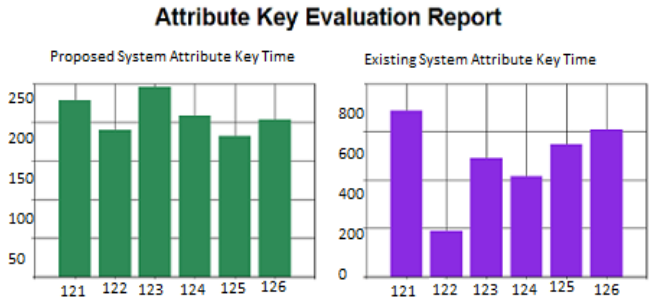

Figure 2: Evaluation Report

5. CONCLUSIONS

EHR services are required to ensure secure and authorized access of patient data. At the same time, they must be able to automatically delegate access of patient data to various caregivers to deliver timely treatment to patients. Security of cloud based EHR services is especially challenging since they are often accessed remotely by the end users.

We have developed a novel, secure, attribute-based authorization mechanism for EHR services that uses Attribute Based Encryption to encrypt the patient records and allows for delegated secure access of patient records. Also, this mechanism transfers management overhead from patient to the medical organization and allows easy access to medical providers.

Thus, the implemented system requires lesser time for attribute key generation as it is not user specific. Also, to improve the security of the document, Hybrid Encryption algorithm is used. In hybrid encryption algorithm, a combination of AES and RC6 algorithm is proposed.

REFERENCES

[1] Wing P, Langelier M, Continelli T, Armstrong D. Data for decisions: The HIM workforce and workplace - 2002-member survey. Chicago: American Health Information Management Association. 2003.

[2] Sittig DF, Singh H. Defining health information technology - related errors: New developments since To Err Is Human. Arch Intern Med. 2011; 171(14): 1281-4.

[3] K. H¨ayrinen, K. Saranto, and P. Nyk¨anen, "Definition, structure, content, use and impacts of electronic health records: a review of the research literature," International journal of medical informatics, vol. 77, no. 5, pp. 291–304, 2008.

[4] Mirani N, Ayatollahi H, Haghani H. A survey on barriers to the development and adoption of electronic health records in Iran. Journal of Health Administration. 2017; 50(15); 3.

[5] Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: Vision, hype,

and reality for delivering computing as the 5th utility. Future Generation computer systems. 2009; 25(6): 599-616.
[6] Kanagaraj G, Sumathi AC. Proposal of an open-source Cloud computing system for exchanging medical images of a Hospital Information System. In Trends in Information Sciences and Computing (TISC), IEEE 3rd International Conference, 2011 144-9.
[7] United States Department of Health & Human Services. Health Information Privacy, 2011.
[8] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina. Controlling data in the cloud: outsourcing computation without outsourcing control. In Proceedings of the 2009 ACM workshop on Cloud Computing Security, CCSW '09, 2009.
[9] M. Joshi, S. Mittal, K. P. Joshi, and T. Finin, "Semantically rich, oblivious access control using abac for secure cloud storage," in Edge Computing (EDGE), 2017 IEEE International Conference on. IEEE, 2017, pp. 142–149.
[10] 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, 2016.
[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security. Acm, 2006, pp. 89–98.
[12] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Security and Privacy, 2007. SP'07. IEEE Symposium on. IEEE, 2007, pp. 321–334.
[13] 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," in Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices. ACM, 2011, pp. 75–86.
[14] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in Proceedings of the 2009 ACM workshop on Cloud computing security. ACM, 2009, pp. 103–114.