ISSN 2320 -2610
Volume 9, No.3, May - June 2020
International Journal of Multidisciplinary in Cryptology and Information Security
Available Online at http://www.warse.org/IJMCIS/static/pdf/file/ijmcis02932020.pdf
https://doi.org/10.30534/ijmcis/2020/02932020

Cloud Based Electronic Health Record Security by Using Image Encryption

Athira P[1], Sayana Safees[2], Vaishnavi Biju[3], Simy Mary Kurian[4]
[1]Department of Computer Science and Engineering, India, athira0718@gmail.com
Department of Computer Science and Engineering, India, vaishnavinadapprayil@gmail.com
[3]Department of Computer Science and Engineering, India, sayanasafees93@gmail.com
[4]Department of Computer Science and Engineering, India, simy.kurian@mangalam.in

ABSTRACT

Each and every one of us are sure to have been in hospital for the health maintenance. It is inappropriate for us to go to the same doctor every time, so each time we need to give our previous health status, the allergetic medicines, the blood report etc. to the doctor we meet, and it is not obvious that we may remember the name of medicines and reports. What if all these things are recorded and stored in a database that could be accessed from anywhere for the accurate medical treatment. Here it is, the paper introduces a cloud based electronic health record security by using image encryption which is a so called data base to store the health status, reports etc. This is made with an easy access technology as stored in a cloud so as to access it whenever necessary. However, it has recently notified about the hospitals keeping the patient record and providing it for further checkups which help in the analysis of the patient more precisely where as it could be accessed by those respective hospitals only. Thus, a new idea of developing these records into a cloud could make it accessible anywhere in the world when a patient is admitted. This provides an easy way to the bystander too if they are unaware of the health status and medicines used by the patient. The security issues related to the patient details are encrypted with attributes related to it.An electronic health record is provided with attribute-based encryption to provide the secure entry of the individual. The individual could be accessed to it using a unique id or mobile num.

Key words:Attribute based Encryption, EHR-Electronic Health Record.

1. INTRODUCTION

The recent past has seen an increased adoption of cloud based EHR services. 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. Various research efforts have been proposed with major focus on secure, cloud-based EHR systems. However, majority of the proposed approaches lack in guaranteeing an attribute-based access control and encryption mechanism. The focus of n multiple data owner scenario and divide the users in EHR system into multiple security domain.Our system can be used by medical organizations for securely maintaining EHRs, at a very low operational cost.

We intend to use the sha256 algorithms and AES platform used as the algorithm provide more reliable platform and efficiency in the encoding of cryptography. The mechanism used here transfers the service management overhead from the patient to the medical organization and allows easy transfer of cloud-based EHR's access authority to the medical providers.

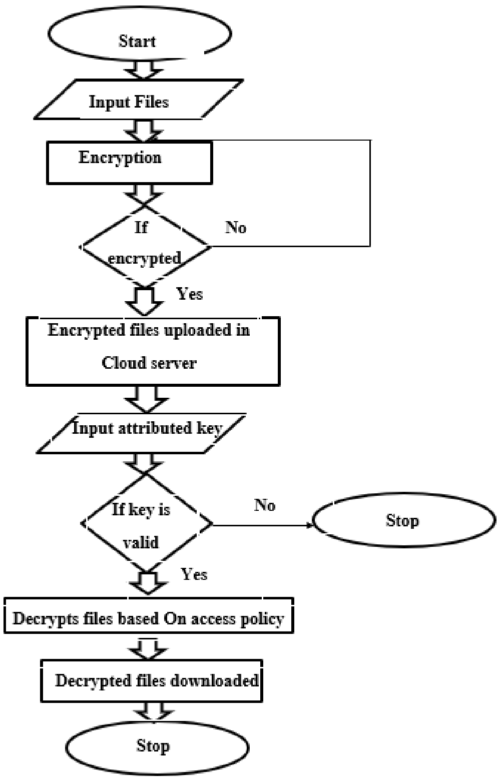


Figure 1: Block diagram of secure EHR

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. This system can be used by all medical organizations for securely maintaining EHRs of a patient at a very low operational cost. It incorporates a semantically rich, policy-based approach using Attribute Based Access Control (ABAC). Further, to guarantee a tight data security, we use Attribute Based Encryption (ABE) at a field-level to encrypt and store the patient EHRs.

1.2 EHROverview

EHR is an Electronic Health Record that helps to keep a patient record in a cloud and helps them to get a record of the health condition of the person and get access from anywhere.
It allows a patient to create, manage and control their personal health data in one plane through the web service or an application, which has made the storage retrieval and sharing of the medical information more efficient EHR's encryption uses the Attribute Based Encryption (ABE) technique. The focus is in multiple data owner scenario and divides the users in EHR system into multiple security domains. An Electronic Health Record (EHR) is an electronic document that details all the relevant clinical reports of a person, over a period of time.

2. LITERATURE SURVEY

2.1 Patient Controlled Encryption: Ensuring Privacy ofElectronic Medical Records

The electronic health record faces many privacy issuesmedicaldata is also miss use forearning profit from it. The accesscontrol method guaranteeing privacy in our medical information. In thiscontrol technique provide verification of any party accessing apatient's health care record. It also keeps communications, log of all access. In this systemseparately store decryption keysin the server itself patient details. Thesetechniques provide strong securities. Cryptographicstorage file system reduces the no of keys for store and retrieve. In an EHR system We can store and retrieve all medical information, it can access family, friends and designated healthcare providers.

Hierarchical health efficient access to patient main class subdivided in to subclass. It also provides accessibility ofsubclasses. patient'srecord is stored as a collection ofentries, entry contains the name of a file, the name of thesmallest category containing that file a locator tag which isused to refer the file.PCE system consist of four algorithms PCE key Gen whichgenerates a root secret and a public key for the patientsPCE key Der which takes a secret key for sub category, Ecn for encryption algorithm which takes a public key and secret key, Dec for decryption algorithm.Two important properties are correctness and correctnesswhich assert that any correctly encrypted document. Securitywhich says encryption of a document in a given category.Search ability of an encrypted algorithm is anotherImportant property. Databaseconsists of encrypted string.[1]

Theserver can determine if the query string matches any string indatabase. In search ability include four additional algorithms.Search key Gen generate a root secret key and a public key,search key Der that takes a searching secret key for index GenUsed for index generation, Trap which is used to decryptionKey for a category and keyword. Health record uses public key and symmetric key schems.ithas both advantage and dis advantage. Symmetric key provideefficiency searching.This system provides uploading without key distribution flexible Hierarchic, high efficiency, easy to add categories.

2.2 Role-Based Access Control Models

We can relate this word in the field of cyber security. Mainly roles played in individual users with in an organization as the basis of governing their access to its network and resources. In other words, it is arole-based security approach to restricting system access to authorized users.It is used by the majority of enterprises with more than 500 employees. Providing rights or access job related tasks such as viewing, creating or modifyingdocuments.RBAC is member from the family of permission management. And origin from old multi user computer systems.

Benefits: In companies itdecreases the need of paper works and password changes when they hire new employees or switch the roles of existing employees.RBAC gives network administrators and managers more visibility and oversight into the business. Implementing RBAC means restricting access to sensitive information, thus reducing the potential for data breaches or data leakage. RBACresearch is still in progress.

2.3 Securing electronic medical records using attribute-based encryption on mobile devices

This is a design and implementation of self-protecting electronic medical records (EMRs) usingattribute-based encryption on mobile devices. The system allows the healthcare organization to export EMRs to location outside. The solution is designed to maintain the EMR availability even when the providers are in offline. The system is designed to provide a fine-grained encryption and able to protect the individual items within an EMR to balance the needs of emergency care and patient privacy.[2]

Each encrypted itemhas its own access control policy. The system implemented a prototype using a new-key and ciphertext-policy attribute-based encryption library as developed There are multiple, parallel efforts could be taken for modernize the medical record system for greater efficiency, improved patient care, patient privacy, and cost savings.[3,13]

There are many benefits from the electronic medical records (EMRs), that is lab tests, images, diagnoses, prescriptions and medical histories of the patient. The EMRs offers that the great privacy and better access to records when they are needed. For the quicker access the more patients and physicians are shifting towards accessing EMRs via in their mobile devices. These devices are used in myriad environment and simultaneously access multiple networks, they have wide exposure of attacks.

This Work is utilizing with the Attribute Based Encryption. The ABE is a form of public key encryption, meaning that any party can encrypt. The corresponding private keys are generated by a trusted party known as the Private Key Generator (PKG). By offline access the system is designed to enable the secure export of EMR in hospital's trust boundary and which includes EMR's that are held by patients by a mobile device [4,14].

The system implementation is done by Policy Engine that is a Python-based policy engine that evaluates EMRs based on CCR-compliment metadata. This policy engine produces an encryption policy and a policy visualization.

It shows how the system enables the realistic use cases such as treatment of minors and advanced directives. The policies are specified the ABE Keys are used to encrypt fields in the EMRs to restrict who can read the data. As it provides a proof-of-concept mobile app that allows patients to access the encrypted records on their iPhone offline and security export those records on other cloud-based EMR Providers.

2.4 Cipher Text-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization

Public-Key encryption is a powerful mechanism for protecting the confidentiality of stored and transmitted information. Traditionally, encryption is viewed as a method for a user to share data to a targeted user or device While this is useful for applications where the data provider knows specifically which user he wants to share with, in many applications the provider will want to share data according to some policy based on the receiving user's credentials.[5]

A user's private key is associated with a set S of attributes and he will be able to decrypt a cipher text if his attributes satisfy " the access matrix associated with the ciphertext. Our main tool to prevent this is to randomize each key with a freshly chosen exponent t. During decryption, each share will be multiplied by a factor t in the exponent. Intuitively, this factor should bind" the components of one user's key together so that they cannot be combined with another user's key components. During decryption, the different shares (in the exponent) that the algorithm combines are multiplied by a factor of it. Ultimately, these randomized shares are only useful to that one particular key.

2.5 Privacy Preserving EHR System Using Attribute-Based Infrastructure

Secure Management of Electronic Health Records (EHR) in a distributed computing environment such as cloud computing environment such as cloud computing where computing resources including storage is provided by a third-party service provider is a challenging task. the paper provides the explore techniques which guarantees security and privacy of medical data stored in cloud. Because of the sensitivity of the health-relatedinformation, provide secure storage and access to EHR is the main challenges in today's EHR systems. patient's privacy has been recognized in law, and privacy law such as the health insurance portability and accountability act (HIPAA) privacy and security rules, and personal information protection and electronic documents act for health data are aimed at ensuring sufficient care is given to handling such data.[6,15]

An increasingly popular approach in managing health data puts users at the center of such systems and allows users to store and manage access to their own health information. Patient-centric EHR systems enables patients to selectively gives access to their health data to healthcare providers and other. The paper shows a secure design for a patient centric EHR management system where data is saved in a storage provided by a cloud provider. This means that it is the responsibility of the user to provide mechanisms that ensure security and privacy of their information. The storage provider will not be able to see data, or associated metadata, therefore confidentiality and privacy of data will be guaranteed. The scheme presented can also be applied to other general security-sensitive database applications. The proposed system ensures the users of the system are patients and healthcare providers that is doctors, laboratories and pharmacists. [7,16,17]

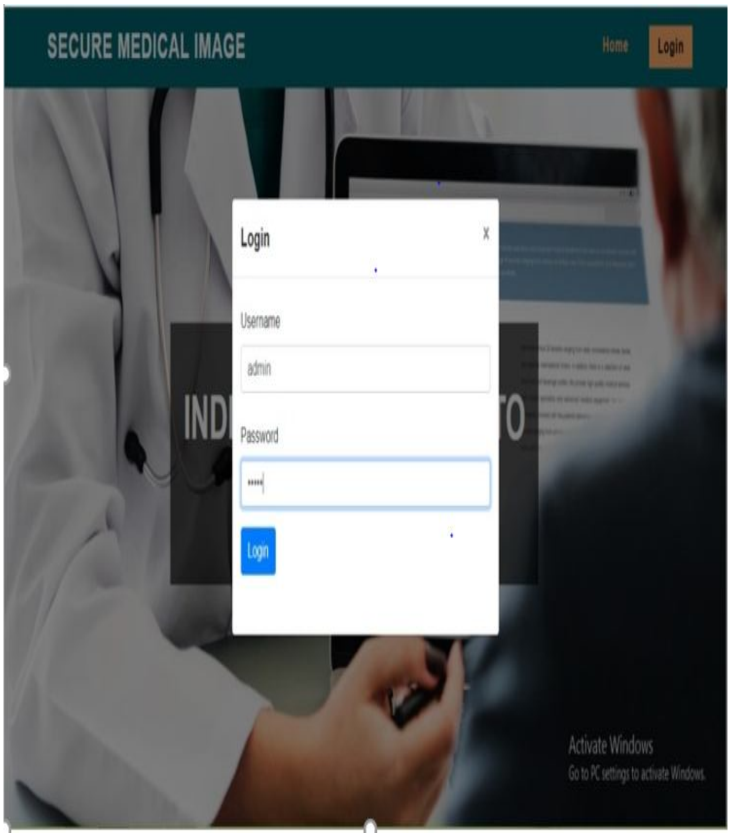
It requires the EHR system to guarantee the confidentiality of health data in storage and transits. By the confidentiality means the cloud provider will not be able to read patient's file contents. An ABE system is a public key encryption system in which user's key is labeled with a set of attributes and the cyphertext is associated with an access policy.[8] The secret key of the user can decrypt a particular ciphertext only if the attribute set of the user's key satisfies the access policy associated with the cyphertext. Such an ABE is known as ciphertext-policy ABE. There are many other functionalities performed by EHR systems that is Adding User-access, Revoking User-access, AccessDelegation, KeywordSearch, Security and Privacy. The Preliminaries are the Health record structure, UserAttributes, Access policies and Attribute-based cryptography [9]. The Health record structure is the patient health record is composed of various health data pertaining to different areas such as dentistry, cardiology, mentalhealth, physical data summary etc.

A patient may want to share his record to a doctor but may not want to allow others to read any more information than strictly necessary. Therefore, the proposed system in which a patient can grant access to specify portions of the health data. The system decides the patient access his health data and thereby determines the attribute set under which the resource is encrypted. The Attribute based cryptography based on 'attributes' of users and objects, and not their individual identities can still be used as one of the attributes. The Analysis is the Efficient Key Management, Direct Revocation and Usability. The proposal ensures the confidentiality of health data by the means of using strong encryption primitive. In this case, the use of adaptive chosen ciphertext secure broadcast ciphertext-policy attribute-based encryption and public-key searchable encryption. This implies if the health record database is compromised the adversary learns nothing about the health data contained in the server without the relevant private keys. Since the system requires a trusted authority to issue the keys, the security of the system relies on the trust and reliability of the authority.[10] The Attribute - based cryptographic primitives provides flexible policies which can be used to build secure infrastructure for designing privacy preserving electronic health record system.

The system develops a prototype of the proposed EHR system using Indigo an open source software developed for patient-centric health record management. It also intends to extend our proposed solution to support multiple authorities to reduce the trust requirement in the key generators.

3. PROPOSED MODEL

The system is guaranteed the confidentiality of health data in storage and transit. By confidentiality we mean the cloud provider or an adversary will not be able to read patients' files privacy of data. By privacy, we mean that the cloud provider will not be able to infer information about the file's content other than what is revealed through the file size and attributes.



Username
admin
Password
•••••

Figure 2: User Login Preface

The secure login phase of the user appears as this interface.
An EHR can be seen as a directory of files stored in subfolders. We assume an electronic health record has the following structure:

(i) Patients' health data in the form of files (in encrypted form)

(ii) A table consisting of entries corresponding to the files.

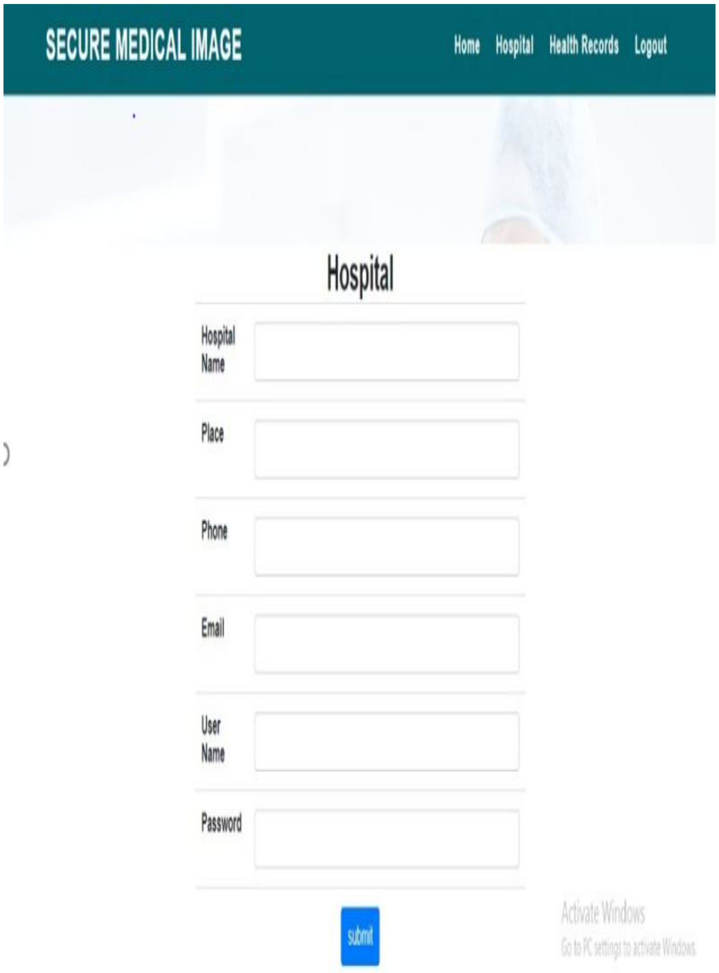


Figure 3: Entry form of the patient

4. EXPERIMENTAL RESULTS

The experimental studies on the topic show the greater exposure of treatment in the medical field. The detailed entry of a person's health history provides more beneficial to the self-analysis by themselves and prediction on their health and hoe to maintain a healthy life.

When we look into the medical research area it helps the doctors and the medical representatives to deal with the person more conveniently than looking on to the person from the beginning.

The previous analysis of the data allows them to provide accurate way of treatment and check on to the allergic part of the medicine if any.

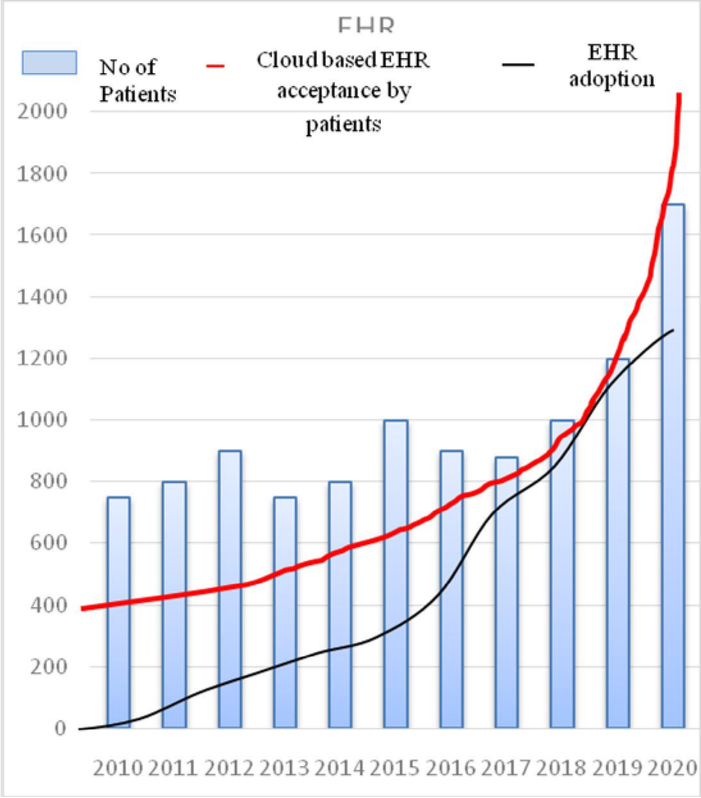


Figure 4: EHR acceptance

Looking into the graph of the EHR it shows the patient's acceptance on the cloud basedEHR in the medical field with that of the existing system. Here we can see the gradual increase in the usage of Electronic Health Record but still many are not accepting the EHR usage due to the security issues related to the breach of information.

There we make use of the image encryption provided for the better security of personal details.

5. CONCLUSION AND FUTURE SCOPE

The Electronic Health Record is being integrated into the cloud for the easy access of the health department to query on the patient. This helps them for the easy assessment based on the health history and medical details.TheAttribute Based Encryption standard helps to provide a security to the patient details. It also makes a relief to the bystander even if they don't know about the medical status of the patient.The future scope is that it could be made an access grant through the fingerprint security if the patient is unconscious also the individual could gain an entry to look into the profile at their fingertip through an android app in their smartphone, which could also help the person to notify about the medicine on timely basis.

REFERENCES

1. R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman**Rolebasedaccess control models**
2. B. Waters,**Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization** in *International Workshop on Public Key Cryptography*.
3. 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**
4. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter**Patient controlled encryption: ensuring privacy of electronic medical records**
5. S. Narayan, M. Gagn´e, and R. Safavi-Naini**Privacy preserving EHR system using attribute-based infrastructure**
6. J. A. Evans, **Electronic medical records system.**
7. E. H. Shortliffe**The evolution of electronic medical records**
8. M. Lavin and M. Nathan, **System and method for managing patientmedical records**
9. M. Joshi, S. Mittal, K. P. Joshi, and T. Finin,**Semanticallyrich,oblivious access control using abac for secure cloud storage**
10. K. P. Joshi, Y. Yesha, and T. Finin, **An ontology for a hipaa compliantcloud service**in *4th International IBM Cloud Academy ConferenceICACON 2016.*
11. V. Goyal, O. Pandey, A. Sahai, and B. Waters, **Attribute-based encryption for fine-grained access control of encrypted data**
12. R. Zhang and L. Liu, **Security models and requirements for healthcare application clouds** in *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on.*

13. Vinodh P Vijayan, Deepti John, Merina Thomas, Neetha V Maliackal, Sara Sangeetha Varghese **“Multi Agent Path Planning Approach to Dynamic Free Flight Environment”**, International Journal of Recent Trends in Engineering (IJRTE), ISSN 1797-9617 Volume 1, Number 1, May 2009, Page(s): 41-46.

14. Juby Joseph, Vinodh P Vijayan**” Misdirection Attack in WSN Due to Selfish Nodes; Detection and Suppression using Longer Path Protocol”** International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 7, July 2014, pp. 825-829, ISSN: 2277 128X

15. V P Vijayan, Biju Paul **“Multi Objective Traffic Prediction Using Type-2 Fuzzy Logic and Ambient Intelligence”** International Conference on Advances in Computer Engineering 2010, Published in IEEE Computer Society Proceedings, ISBN: 978-0-7695-4058-0, Print ISBN: 978-1-4244-7154-6

16. Vijayan V P, Gopinathan E **“Improving Network Coverage and Life-Time in a Cooperative Wireless mobile Sensor Network “** Fourth International Conference on Advances in computing and communications (ICACC) Aug, 2014. Published in IEEE Computer Society Proceedings. Print ISBN: 978-1-4799-4364-7, INSPEC AccessionNumber:14630874,DOI:10.1109/ICACC.2014. 1 6 PP 42-45.

17. Vinodh P Vijayan, Biju Paul **“ Traffic scheduling for Green city through energy efficient Wireless sensor Networks ”** International Journal of Advanced Trends in Computer Science and Engineering, Volume 8, No.4, July – August 2019, ISSN 2278-3091, https://doi.org/10.30534/ijatcse/2019/81842019.