CIPHER TEXT POLICY ATTRIBUTE BASED ENCRYPTION FOR SECURING PATIENT HEALTH RECORDS

Dr.P.Veeralakshmi,
Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India

Abstract—The Electronic health record (EHR) system is an emerging patient-centric model of health information, which is sent to store information at a third party, such as cloud providers. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to EHRs stored in semi-trusted servers (cloud). To achieve fine- grained and scalable data access control for EHRs, we use Ciphertext policy attribute based encryption (CPABE) techniques a kind of attribute Based Encryption (ABE) to encrypt each patient's related EHR information. This scheme also enable dynamic modification of access policies, also supports efficient on-demand attribute revocation and break-glass access under emergency scenarios using the Ciphertext policy attribute based encryption (CPABE). The new scheme provides access control and encryption features embedded into a single algorithm. This project presents the implementation details of a new EHR system with enhanced security using CPABE. The project also proposes another EHR system with improved security.

Keywords:- Cloud Computing, Electronics Health records, Attribute Based encryption, Ciphertext policy based encryption, Partially Hidden Access Structure, Dual System Encryption.

INTRODUCTION

In recent years, the system of Electronic health records (EHR) has emerged as a patient-centric model of health information exchange. An EHR service allows a patient to create data, manage and control their personal health data in a centralized place through the web from anywhere and at any time, which has made the storage of information, retrieval and sharing of the medical information more efficiently easily. Specially where each patient has the full control of his/her medical records and can effectively share his/her health data with users, including staffs of same organization from health-care providers, family members or their friends. Thus in this way the accuracy and quality of care are improved. The cloud computing had a lot of attention because it provides Storage-as-a-Service and Software-as-a-Service, by which software service providers can enjoy the virtually infinite and elastic storage and computing resources. As such, the EHR providers are more and more willing to shift their EHR storage and application services into the cloud instead of building specialized data centers. For example, as two major cloud providers like Google and Microsoft are both providing their EHR services, Google Health [15] and Microsoft Health Vault [16] respectively. While it is exciting to have EHR services in the cloud for every user such that the many security and privacy risks which could impede its wide adoption. The Health Information Technology for economic health (HITECH) Act [19] provides a federal incentive to encourage US healthcare provides to adopt and use EHR systems meaningfully to improve healthcare quality.

[17] The main concern is about the privacy of patients" personal health data who could gain access to the EHRs when they are stored in a cloud server. By these patients lose their physical control to their own personal health information where it is directly placing those sensitive data in the control of the servers cannot provide strong privacy assurance at all. The EHR data could be leaked if an insider/user in the cloud providers organization misbehaves due to the high value of the sensitive personal health information (PHI).

Benefits of EHR

Electronic Health Record (EHR) can be defined as the electronic record that stores patients medical history information in a health record which can be accessible and managed by the care providers and patients. Health record has been in existence for over twenty years now but its use has

been restricted to few healthcare institutions due to high implementation cost in society. The benefits of electronic health records (EHR) outweigh paper records and thus make it the obvious option for storing patient records.

As the health care providers begin to use EHRs and set up ways to securely share patients health information with other users, it will make it easier for every user to work together to make sure patients are getting the cared like as,

- Information about a patients medications will be available in EHRs so that health care providers dont give to patients another medicine that might be harmful to patients.
- Electronic Health Record systems are backed up like in most computer systems, so as a result someone is in an area affected by a disaster, like a hurricane, the health information can be retrieved.
- EHRs can be available in an emergency. If someone in an accident and are unable to explain ones health condition or history of patient, in that situation a hospital that has a system may be able to talk to their doctor's system. The hospital will get information about the peoples medications, health issues, and tests, and hence decisions about someone in emergency care are faster and the doctors are more informed.

The Healthcare organizations must manage information as an asset and have to adopt proactive decision making and oversight through information asset management, information governance to achieve data trustworthiness.

1. USING EHR OVER A CLOUD

The Cloud computing offers significant benefits to the health care sectors like in doctors clinics, hospitals, and health clinics which require quick access to computing and large storage facilities which are not provided in the previous settings. However healthcare data needs to be shared across various settings and geographies which further burden the healthcare provider and the patient causing delay in treatment and loss of time. Thus, Cloud caters to all these requirements thus providing the healthcare organizations an incredible

Doctors using EHRs may find it easier or faster to patients your lab results and share progress with the patient. If the doctors systems can share information, one doctor can see test results from another doctor, and so the test doesnt always have to be repeated, especially with x-rays. This means they are at less risk from radiation and other side effects. Although there exist administrative regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) [18], technical protections that effectively ensure the confidentiality of and proper access EHR are still indispensable.

There are a number of existing rules and regulations on documentation principles and guidelines that primarily address documentation authorship principles [3], auditing, and forms development in the health record. Some of proposed guidelines are being sought by the healthcare industry that ensure and preserve documentation integrity in an age of electronic exchange and changes in the legal evidentiary requirements for electronic business and health records.

Data quality and record integrity issues must be addressed before widespread deployment of health information exchange (HIE). Poor data quality will be amplified with HIE if incomplete, redundant, or untrustworthy data information and records are allowed to cascade across the healthcare system.

opportunity to improve services to their customers, the patients to share information more easily than ever before and improve operational efficiency. Cloud computing comes into focus only when we think about what IT always needs a way to increase capacity or add capabilities on the fly without investing in infrastructure even in training new personnel or providing license to new software. The some of characteristics define cloud data and its applications services:

- Remotely hosted: Services or data are hosted on someone else infrastructure.
- Services or data are available from anywhere.
- Co modified: The result is a utility computing model similar to traditional that of traditional utilities like gas and electricity as they pay for what they would like.

1.1 Challenges and Issues in moving towards cloud Computing

Some of the companies are increasingly awarded about their challenges are as follows.

Security and Privacy- The main challenge to cloud computing is the way it addresses the security and privacy concerns of businesses planning to adopt the same. The Hacking and some of the various attacks to cloud infrastructure would affect multiple clients even if only one site is attacked.

Service Delivery and Billing- It is difficult to assess the costs involved due to the on-demand nature of the services.

Interoperability and Portability- Businesses should have the leverage of migrating in and out of the cloud and switching providers whenever they want, and there should be no lock-in period. Cloud computing services should have the capability to integrate smoothly with the on-premise IT.

Reliability and Availability- Cloud providers may lack round-the-clock service resulting in frequent outages. It is important to monitor the service being provided using internal or third-party tools. It is vital to have plans to supervise usage, SLAs, performance, of these services.

Performance and Bandwidth Cost- Businesses can save money on hardware, but they have to spend more for the business value that cloud computing brings and are taking steps towards transition to the cloud environment. The smooth transition entails a thorough understanding of the benefits as well as the challenges involved. Some of the most important band width. This can be of lower cost for smaller applications but can be significantly high for the data-intensive applications. Delivering intensive and complex data over the network requires sufficient bandwidth.

1.2 Security over cloud

Cloud computing is an efficient technique by which the user can access any data from anywhere and anytime through internet. Thus it is providing a new world of computing technology to the world. When this information is accessed by users, business logic which can limits unauthorized access to users with the proper credentials. Hence to protect against this vulnerability some of the sensitive data should be encrypted when it stored in the database. These encryption and decryption processes create processing overhead and the non- sensitive data should be stored in the clear to minimize costs. Additionally, it should be made sure that any required data indexing is not broken in the encryption process. The some applications which can used for cloud storage like Microsoft Sky drive, Dropbox, Google drive etc which can provide more security for the information which is stored in that.

1.3 Using EHR over cloud

"Patient centricity" has become the key trend in healthcare provisioning and is leading to the steady growth in adoption of electronic medical records (EMR), electronic health records (EHR), personal health records (PHR), and some of the technologies leads to integrated care, patient safety and clinical decision support. Availability of data, has become the key to both patient satisfaction and improved clinical outcomes.

1.4 Need for security in EHR systems

EHRs are electronic versions of the files in a doctors or other health care providers office. An EHR may include a patients medical history, notes, and other information related to the health including the symptoms, diagnoses, immunizations, and reports of tests such as x-rays.

Providers are working with other doctors, hospitals, and health plans to find ways to share that information. This information in EHRs can be shared with other organizations involved in health care if the computer systems are set up to talk to each other. Hence these records should only be shared for authorized users by law or by the patient.

Cloud Computing offers eHealth systems the opportunity to enhance the features and functionality that they offer. However moving patients medical information to the Cloud implies several risks like security and privacy of sensitive data in health records. Hence to protect the confidentiality of patient information and facilitate the process, health care providers must ensure proper security.

The some of the possible security measures that can be built into EHR systems,

- Access control tools like passwords and PIN numbers, to help limit access to your information to authorized individuals.
- Encrypting the stored information like the health information of the patient cannot be read or understood except by those using a system that can "decrypt" it with a "key."
- audit trail feature, which records who accessed certain information, what changes were made and when.
- To overcome the challenges of preserving patients‟ privacy in electronic health record systems, security in the systems should be enforced via encryption as well as access control. So that the patients‟ privacy is protected should the host data center be compromised [2].

2. PRIVACY IN EHR SYSTEMS

The EHR systems typically fall into two categories: cloud- based or client-server. Cloud-based systems store the data on external servers where they can be accessed via the web requiring only a computer with Internet connection in order to access the data. Alternatively, client-server systems store the data in house, requiring a server, hardware and software to be installed for their usage. While more practices are switching to the cloud for a number of reasons which is required. The six benefits for switching to cloud-based systems can be listed as Security, Privacy, Cost effectiveness, accessibility, Reduced IT Requirements, Grows with You.

2.1 Security mechanisms

Encryption "encodes" or "scrambles" data into an "unreadable" form to ensure secrecy. In the view of the advantages in switching over to a cloud environment, it is important for an EHR to address the issues of security of the EHR systems on a cloud. Security mechanisms like encryption and access control need to be implemented to provide security in the EHR systems. The security mechanisms which can studied as below.

Usually Ciphers have used information contained in secret keys to code and decode information or text. The process of coding plaintext to create ciphertext is called encryption and the vice versa is called decryption. The some of the modern systems of electronic cryptography use *digital keys* (bit strings) and mathematical algorithms (encryption *algorithms)* to encrypt and decrypt information. There are two types of encryption as symmetric key encryption and public (asymmetric) key encryption.

- Symmetric key encryption - The symmetric key is also called a secret key because it is kept as a shared secret between the sender and receiver of information otherwise the confidentiality of the encrypted information is compromised between two parties. A prior shared secret should be established by an authenticated and private communications channel before it can be used in the cryptosystem. Some of the examples for symmetric key encryption are AES, DES, Two fish, Serpent, Blowfish, CAST5, RC4, 3DES, Skipjack, Safer+/++ etc.[20].
- Public (asymmetric) key encryption- The protocol is now known as Diffie-Hellman key exchange, or Diffie-Hellman-Merkle key exchange. This discovery was considered a breakthrough in the field of Public- Key Cryptography where encryption and decryption keys are different. Public-key cryptosystems are also referred to as asymmetric cryptosystems. The public key encryption is one in which there are two keys namely a public and a private key used for encryption and decryption. The public and private keys are computed such that they have certain mathematical properties which can satisfy. If the encryption is performed using the public key, the decryption of that cipher is possible only when user using the corresponding private key and if the encryption is performed with the private key, the decryption of the same is possible only with the corresponding public key, which gives a fundamental picture about public key cryptography.

- **Identity Based Encryption (IBE) -** Problems with the traditional Public key cryptosystems (PKCs) are the high cost of the infrastructure needed to manage, authenticate public keys. An Identity-based cryptosystem is a novel type of cryptographic scheme proposed by Shamir [23], which enables any pair of users to communicate securely and to verify each others signatures without exchanging public or private keys, without keeping any key directories and without using the services of any third party.

In view of this, Sahai and Waters [4] proposed a fuzzy IBE scheme, in which some error around the chosen identity can be tolerated. In 2005, Sahai and Waters proposed a system [4] in which a sender can encrypt a message specifying an attribute set and a number 'd', such that only a recipient with at least „d" of the given attributes can decrypt the message.

- **Attribute Based Encryption (ABE) and its enhancements-** ABE [3] is actually a generalization of IBE (identity based encryption). In IBE system, ciphertexts are associated with only one attribute (i.e. identity). Secrecy of communication has been a concern of people since ancient times. Attribute- Based Encryption (ABE) has become a huge area of research in cryptography over the past few years. The concept of attribute based encryption was introduced by Amit Sahai and Brent Waters in 2004 [21, 22] .It is a type of public-key encryption in which the public key of a user and the ciphertext are dependent on the attributes of the user. In such systems, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext.

ABE enables public key based one-to-many encryption and provides promising cryptographic primitives for realizing scalable and fine-grained access control systems.

In an ABE system, a users keys and ciphertexts are labeled with sets of descriptive attributes. The particular key can decrypt a particular ciphertext only if there is a match between the attributes of the ciphertext and the users key which is using during operation. In ABE, a key authority is considered to be a trusted party who generates keys for users within a system. This key authority has a master secret key (MSK) and public key (PK). For every user in the system, the key authority generates keys based on the users attributes, using the *MSK* and each of the user is then given their corresponding secret key, *SK*. When a user wants to encrypt a file data or a related document they construct a policy for that document. There are two kinds of Attribute Based Encryption Schemes as Key-policy ABE (KP-ABE) and Ciphertext-policy ABE (CP-ABE) [5] schemes. Goyal-et al. [7] Proposed a KP-ABE scheme which supports any monotonic access formula consisting of AND, OR, or threshold gates.

The roles of the ciphertexts and keys are reversed in the ciphertext-policy ABE (CP-ABE) introduced by Be then court, Sahai and Waters [5]. In this the ciphertext is encrypted with an access policy chosen by an encryptor but a key is simply created with respect to an attributes set. Subsequently, Cheung and Newport [6] proposed a CP-ABE scheme in the standard model. Their scheme supports AND of attributes by using different parameters for all three possible cases like positive, negative and wildcard or don't care of every single attribute.

To keep sensitive data of the user confidential against un-trusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. To achieve secured scalable and fine grained data access control in Cloud Computing they used the combination of different types of algorithms like Attribute Based Encryption (ABE), proxy re-encryption, and lazy re-encryption [1].

Solutions for these are based on a recent cryptographic primitive, hierarchical predicate encryption (HPE), enhanced efficiency and the other with enhanced query privacy. In addition to document privacy and query privacy, other schemes include: efficient support of multi-dimensional,

multiple keyword searches with simple range query, allows delegation and revocation of search capabilities [9].

Waters [5] proposed CP-ABE constructions based on a few different pairing assumptions in the standard model which work for any access policy that can be expressed in terms of a linear secret-sharing scheme (LSSS) matrix. This scheme supports both access control and encryption.

2.2 Security implementations of EHR over Cloud

The issue of security and privacy of the EHR makes it unacceptable to patients. Centralized and distributed databases introduce the possibility to access large volumes of patient information in a short period. This also increases the chance of an unauthorized person accessing patient records easily. Acceptance of EHR depends on easy implementation, privacy settings and, good security infrastructure. Thus EHR integration remains a challenge and a serious concern since it is exposed to theft, security violation, and standardization difficulties.

The Current studies [17] focused on encrypting and decrypting health records in a controlled environment without considering how encryption and decryption keys can be distributed in the cloud.

Standard encryption techniques are not well suited for EHR systems, especially in cloud-based settings:

1) Symmetric-Key Encryption (SKE): The techniques like, e.g., AES, are usually efficient but introduce complexity in EHR systems to apply access control which is required. Particularly like healthcare providers use one shared key for encryption and decryption thus, if the shared key is compromised, all EHRs are compromised.

2) Public-Key Encryption (PKE). The some of the techniques like e.g., RSA, provide a secure solution but are not practical for secure EHR storage due to the requirement for an expensive public-key infrastructure (PKI) to be maintained for distributing and managing public keys for all healthcare providers.

It is important to focus on attribute-based access control and encryption in the cloud environment. By using the advanced attribute-based access control and encryption will lead to achieve fine-grained security architecture for the EHR in the cloud computing environment.

A new variant of a cipher text-policy proposed by Laun Ibraim et. Al [8]., comprises attribute–based encryption scheme to enforce patient/organizational access control policies such that everyone can download the encrypted data but only authorized users from the social domain (e.g. family, friends) or authorized users from the professionals domain (e.g. doctors or nurses) are allowed to decrypt it. The confidentiality of personal health records is a major problem when patients use commercial web-based systems to store their health data using traditional access control mechanisms, such as Role-Based Access control. Advanced Cryptography can be used to construct a secure and privacy-preserving EHR system to enable patients to share their data among health-care providers in a flexible, dynamic and scalable manner [8].

In cloud environments, if a data owner wants to share data resources with their users he/she will encrypt those data and then upload to cloud storage service. By using encryption the cloud cannot know the information of the encrypted data. Besides to avoid the unauthorized user accessing the encrypted data in the cloud, a data owner should be able to use the encryption scheme for access control of encrypted data. Some encryption schemes can provide security like type of attribute based encryption schemes that can provide access control over encrypted data is the Cipher text policy attribute-based encryption scheme. Hence it is proposed to use CPABE for EHR security. Using CPABE can provide encryption as well as access control to the encrypted data.

2.3 Motivation

Having observed the advantages of deploying EHR systems over cloud, and after studying the various security mechanisms available that can be used in a cloud environment, this work proposes to use the Cipher text Policy Attribute Based Encryption (CPABE) to be used for an EHR system over cloud. Usage of CPABE can provide access control over encrypted data, which ensures security during storage, and also Confidentiality. This would be a novel approach to be used for enhancing EHR security.

3. CIPHERTEXT POLICY ATTRIBUTE BASED ENCRYPTION

The ciphertext-policy Attribute Based Encryption (CP-ABE) was introduced by Bethencourt, Sahai and Waters [5]. The ciphertext is encrypted with an access policy chosen by an encryptor.

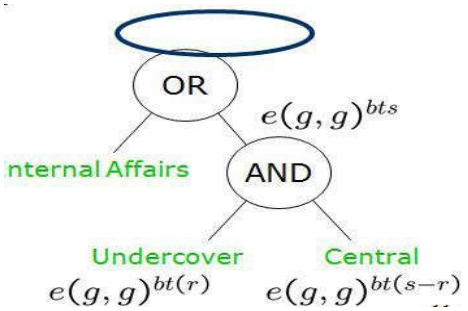


Fig 1: access structure

3.1 Mathematical Background

The Cipher text policy attribute based encryption involves the various mathematical notations which are defined in this section.

3.1.1 Composite Order Bilinear Groups

Definition 1: Bilinear Maps construct a relationship between two cryptographic groups leading to new schemes. (Bilinear Maps): Let *G1* and *G2* be cyclic groups of prime order *p*; *g* a generator of *G1*. *e* is a bilinear map, *e: G1 * G1* □ *G2*, where |*G1*| =|*G2*| = *p*. The bilinear map e has three properties:

1) Bilinearity: *P,Q € G1, a,b € Z*p, e(aP , bQ)* =
2) Non-Degeneracy: *P ≠ 0 => e(P,P) ≠ 1*,
3) Computability: *e* is efficiently computable.

3.1.2 Access Structures

Access structures are used in the security system where multiple parties need to work together to obtain a resource. Groups of parties that are granted access are called qualified sets. The set of all sub qualified sets is called the access structures of the system. Access structures are monotone that if a subset S is in the access structure, all sets that contain S are a subset should also form part of the access structure.

Definition 2: [Access Structure]: Let {P1,…….,Pn} be the set of parties. A collection A subset of is monotone if *B, C*: if *B € C* and *B* subset of *C* then implies *C € A*. An access structure is a monotone collection 1 ***A*** of non-empty subsets of {P1,…….,Pn} . The set in ***A*** are called the authorized sets, and the sets not in ***A*** are called the unauthorized sets. In these recent CP-ABE schemes, the attributes will play the role of parties and only the monotone access structures are dealt with. From now on, unless stated otherwise, by an access structure we mean a monotone access structure.

The recent CP-ABE schemes employ linear secret-sharing schemes and use the definition adapted as shown in above fig 1.

3.1.3 Linear Secret sharing Schemes (LSSS)

This construction employs linear secret sharing schemes (LSSS).

Definition 3: (LSSS). A secret sharing schemes Π over a set of parties P is called linear (over Zp) if

1. The shares from each party form vector over Zp.
2. There exists a matrix A with l rows and n columns called the share-generating matrix for Π. For all I = 1,……,l, the ith row of A is labeled by a party ρ(i). When we consider column vector v= (s, r2 …rn), where s € Zp is the secret to be shared, and r2… rn € Zp are random chosen, then Av is the vector of l shares of the secret s according to Π. The share (Av) I belongs to party ρ (i).

It is shown as [10] which is more flexible and expressive than previous works [11,12,13], that every linear secret sharing scheme according to the above definition also enjoys linear reconstruction property as defined Suppose that in an LSSS for access structure A.Let we say S A be any authorized set, and let I { 1,……,l} be defined as I={i| (i) S}.then there exists a constants. Note that for authorized sets no constant exists.

3.2 Construction

In the actual construction, the private keys will be identified with a set of descriptive attributes. A user who wishes to encrypt a message will specify through an access tree structure a policy that private keys must satisfy to decrypt. The every interior node of the tree is a threshold gate and the leaves are associated with the attributes. The required user will be able to decrypt a ciphertext with a given key if and only if it satisfy set of attributes from the private key to the node of the tree such that the tree is satisfied. The same notation is used to describe the access trees, even though in our case the attributes are used to identify the keys specified in the private key while the cipher texts are simply labeled with a set of descriptive attributes which are required.

The ciphertext-policy attribute based encryption (CP-ABE) scheme consists of four Phases: Setup, Key Gen, Encryption and Decryption as shown. The process of each phase is as follows:

1) **Setup Phase:** The setup algorithm takes security parameter and attributes universe description as input. It outputs the public parameters *PK* and a master key *MK*. The setup algorithm will choose a bilinear group of prime order *p* with generator *g*. Next it will choose two random exponents *α, β Zp*. The public key is published as:

PK = , g, h = , f = ,e

and the master key *MK* is *(β,)*.

2) **Key Generation Phase:** The key generation algorithm takes as input the master key MK and a set of attributes S that describe the key. It outputs a private key SK.

The key generation algorithm will take as input a set of attributes S and output a key that identifies with that set. The algorithm first chooses a random *r Zp,* and then random *rj Zp* for each attribute *j S.*

Then it computes the key as

SK = (D = g (α+r)/β, j S : Dj = gr · H(j)rj ,D'j = grj).

3) **Encrypt Phase**: The encryption algorithm takes as input the public parameters *PK*, a message *M*, and an access structure A over the universe of attributes. The algorithm will encrypt *M* and produce a cipher text *CT* such that only a user that possesses a set of attributes that satisfy the access structure will be able to decrypt the message. We assume that the cipher text implicitly contains *A.*

The encryption algorithm encrypts a message *M* under the tree access structure *T*. The algorithm first chooses a polynomial for each node *x* (including the leaves) in the tree *T*. These polynomials are chosen in the following way in a top down manner, starting from the root node *R*.

- For each node *x* in the tree, set the degree of the polynomial to be one less than the threshold value of that node, that is, = − 1.
- Starting with the root node *R,* the algorithm chooses a random *s Zp* and sets *qR(0) = s.*
- Then, it chooses *dR* other points of the polynomial *qR* randomly to define it completely.
- For any other node *x*, it sets *qx(0) = q parent(x)(index(x))* and chooses *dx* other points randomly to completely define *qx.*

Let, *Y* is the set of leaf nodes in *T.* The ciphertext is then constructed by giving the tree access structure *T* and computing

CT = (T , C' = M e(g, g)αs, C = hs, y Y : Cy = gqy(0),C'y = H(att(y))qy(0)).

4) **Decrypt Phase**: The decryption algorithm takes as input the public parameters *PK*, a cipher text *CT*, which contains an access policy *A*, and a private key *SK*, which is a

private key for a set S of attributes. If the set S of attributes satisfies the access policy structure A of ciphertext then the algorithm will decrypt the cipher text and return a message M. The decryption procedure is a recursive algorithm. For ease of exposition the simplest form of the decryption algorithm is presented.

CPABE is an enhanced encryption scheme providing security at both access control and encryption levels.

4. ENHANCING EHR SECURITY USING CPABE

Electronic sharing of health records promises significant benefits. Ensuring that patients are able to control who has access to what parts of their medical histories is vital to this endeavor. Providers and public health advocates consider in dispensable unfettered access to individual medical records that technology now makes possible. Hence this paper proposes the system architecture for enhancing EHR security using CPABE.

4.1 System Architecture

In healthcare [14], it must meet the requirements of Health Insurance Portability and Accountability Act (HIPAA) [18] for any use or disclosure of protected healthcare information therefore there is no option but to keep medical data confidential against cloud storage servers. Consider the example of following [10] for cloud storage for healthcare information. Suppose that a data owner intends to outsource a medical record to the cloud and specifies that the medical record can only be accessed by a patient with some social security number 013-22-345. The data owner encrypts the record using a CP-ABE scheme in order to keep it confidential from the cloud service provider. If the data owner uses a traditional CP-ABE scheme to encrypt the medical record, everyone including the cloud service provider is able to know the access policy associated with the ciphertext, and can infer that someone with social security number 013-22-345 suffers

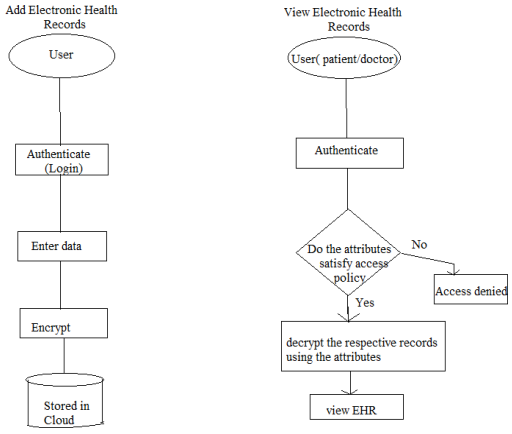


Fig 2: Add and View EHRs

from a heart problem. Hence it is clearly not acceptable and shows the necessity of hiding the access policies from prying eyes in certain applications in existing systems.

A secured framework for patient-centric information and a suite of mechanisms for data access control to EHRs has been proposed. In order to achieve fine-grained and scalable data access control for EHRs, we leverage Cipher-text Policy based Attribute based encryption (CPABE) to encrypt each patients EHR file and use the security policy to allow the access of the data.

We propose an enhanced EHR system by implementing CPABE to ensure security and access control of encrypted data. This unit presents the system architecture and the implementation of the system proposed. During implementation the terms **Public Health records (PHR) and electronic health records (EHR)** are used synonymously.

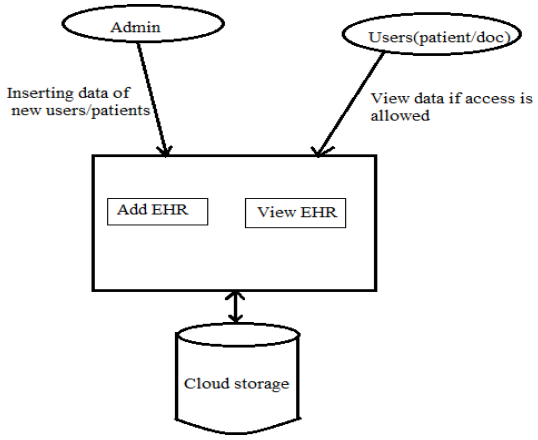


Fig 3: Overview of proposed system in Cloud

In the proposed system, the users (patients/doctors) insert

an EHR if they are the owners or the administrator. The EHR is then encrypted using the attributes of the owner and an access policy, and stored in the cloud.

The EHR is now securely stored on the cloud. To view or update an EHR, the user once authenticated, will be checked for his attributes whether they satisfy the policy specified during encryption/ decryption. If the Conditions are satisfied, the user will be given the appropriate access to the EHR.

From the fig.2 and3 there should be an Administrator or (Admin) who will access all the data of the patients which is stored in the database and also insert the various patients" records in EHR. The admin will be able to encrypt and decrypt the record which is required for the further use or the details. On the other side the patient can also access his information or data only if he/she satisfies his attributes during the decryption time. This information will be stored in the cloud environment using some storage applications and even able to download data from that cloud during the decryption time when it is required. Hence during the decryption time it provides more security as the data will get decrypted only if the required user attributes satisfy, thus making the scheme more flexible.

4.2 Implementation preliminaries

The above proposed system is demonstrated using .Net 4.5, JDK 1.6 using the languages C#, java. The operating system can be window 7 and other compatible version. Visual studio.Net version 2012 and Net beans 6.9.1 are the IDE which are used for this application. For storing the information, the system using *sky drive* a cloud server is being used.

The current implementation includes Cipher text policy attribute based encryption for storing and retrieving the Electronic Health Records. Electronic Health records in this implementation are considered to be either Text files or Image files. The main contribution of the project is the implementation of Ciphertext Policy Attribute based encryption (CPABE) over text files as well as image files.

The implementation of CPABE involves implementation of mathematical notations introduce in unit 4 which needs the Pairing Based cryptography library (PBC library), BSWabe library. CP-ABE allows a sender to disseminate messages according to an access policy which can be expressed as a Boolean function consisting of OR, and between attributes. A receiver whose secret key is associated with those attributes can only decrypt a cipher text successfully if and if only if its attributes satisfy the cipher texts access policy. CPABE involves the following four algorithms which have been implemented and there execution is shown in the form of screenshots.

1) **Setup Phase:** The setup algorithm takes security parameters and attributes universe description as input. It outputs the public parameters *PK* and a master key *MK* as shown in below Fig 4.

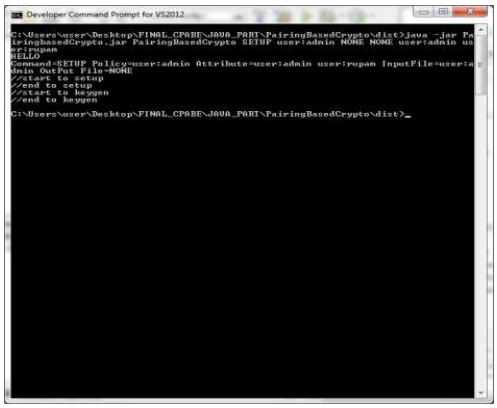


Fig 4: Setup phase in CPABE

2) **Key Generation Phase:** The key generation algorithm takes as input the master key *MK* and a set of attributes *S* that describe the key. It outputs a private key *SK* as shown in fig 5.

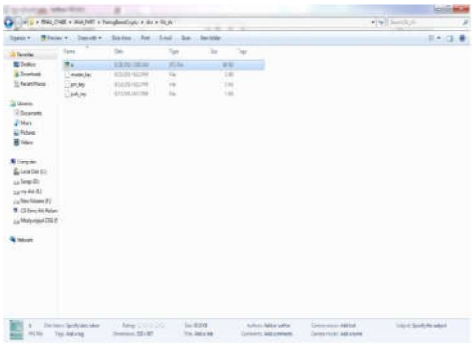
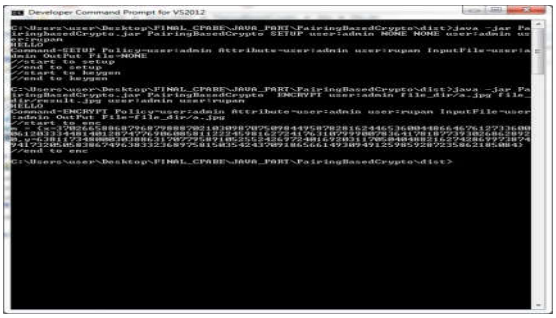


Fig 5: KeyGen in CPABE which outputs *Pub_key, Prv_key, Master_key*

3) **Encryption Phase**: The encryption algorithm takes as input the public parameters *PK*, a message *M*, and an access structure A over the universe of attributes. The algorithm will encrypt *M* and produce a cipher text *CT* such that only a user that possesses a set of attributes that satisfy the access structure will be able to decrypt the message.

An image file (.jpg file) is being encrypted as shown in Fig 6. The encrypted image is unintelligible this is demonstrated in fig 7.



4) **Decryption Phase**: The decryption algorithm takes as input the public parameters *PK*, a cipher text *CT*, which contains an access policy *A*, and a private key *SK*, which is a private key for a set *S* of attributes as in Fig 8. If the set *S* of attributes satisfies the access policy structure *A* of cipher text then the algorithm will decrypt the cipher text or image and return a message *M* or given filename which is decrypted.

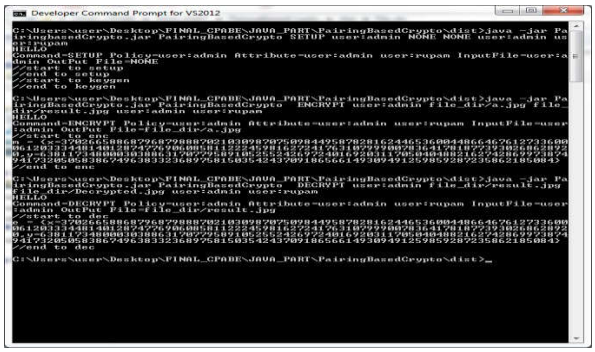


Fig 8: Decryption phase in CPABE

The encrypted image is decrypted in this phase. After running decryption algorithm the new generated decrypted file shown. The contains of the decrypted file are shown in fig 9 which is decrypted image.

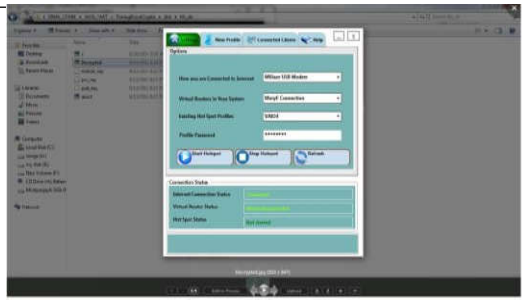


Fig 6: Encryption phase in CPABE

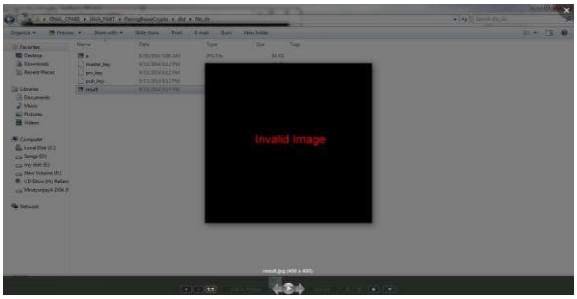


Fig 7: Encrypted Image

It can observe that how the encrypted Image is being stored in the File directory using CPABE.

Fig 9: Decrypted Image

CONCLUSION AND FUTURE WORK

This paper proposes a novel framework of securely sharing Data needs to be stored in an encrypted form on a cloud so as to provide access only to authorized persons. This authorization instead of being managed at a database level, can be provided at the user level, by checking the attributes of the user. The user attributes are used for encrypting the data instead of some other keys to be remembered by the user. Encryption also depends on the access policy to be used for accessing the data. Decryption is also based on the attributes and the policies specified during encryption. The method makes sure that the secret data of the patient is accessed and used by only authorized persons, providing highest level of security.

The main motto of the patient centric model is that the share the personal health records of the patient with maximum.

REFERENCES

[1] Yu, S., Wang, C., Ren, K., Lou, W.: *Achieving secure, Scalable, and fine-grained data access control in cloud computing*. In: IEEE INFOCOM 2010(2010).

[2] Benaloh, J., Chase, M., Horvitz, E., Lauter,K.: *patient controlled encryption Ensuring Privacy of electronic medical records.* In: CCSW 2009: proceedings of the 2009ACM workshop on cloud computing security,pp. 103-114(2009).

[3] M.Chase. Chow, S.S.: *improving privacy and security in multi-authority attribute Based encryption* nicks 2009, pp.121- 130(2009).

[4] A. Sahai and B. Waters. *Fuzzy identity-based encryption*. Advances in Cryptology{EUROCRYPT 2005, pages 457{473, 2005.62}.

[5] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in IEEE Symposium on Security and Privacy, 2007, pp. 321-334.

[6] L. Cheung and C. Newport. *"Provably secure ciphertext policy ABE".* In CCS'07:proceedings of the 14th ACM conference on Computer and communications security,
pages 456–465, New York, NY, USA, 2007.ACM.

[7] Alexandra Boldyreva , Vipul Goyal , Virendra Kumar, *Identity-based encryption with efficient revocation*, Proceedings of the 15th ACM conference on Computer and communications security, October 27-31, 2008, Alexandria, Virginia, USA

[8] Ibraimi, Luan and Asim, Muhammad and Petkovic, Milan (2009) *Secure Management of Personal Health Records by Applying Attribute-Based Encryption.* [Report], CTIT technical report series, July 2009

[9] M. Li, S. Yu, N. Cao and W. Lou, &ldquo,Authorized Private Keyword Search over Encrypted Data in Cloud Computing,&rdquo, *Proc. 31st Int',l Conf. Distributed Computing Systems (ICDCS ',11),*pp. 383-392, 2011

[10] Junzuo Lai, Robert H. Deng and Yingjiu Li, "Expressive CP-ABE with partially hidden access structures", Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security (AsiaCCS 2012), May 2012, Seoul, Korea.

[11] T. Nishide, K. Yoneyama, and K. Ohta. Attribute-based encryption with partially hidden encryptor-specified ccess structures. In ACNS, pages 111–129, 2008.

[12] J.Li, K.Ren, B. Zhu, and Z. Wan. *Privacy-aware attribute-based encryption with user accountability*. In ISC, pages 347-362, 2009.

[13] J. Lai, R.H. Deng, and Y. Li. *Fully secure ciphertext-policy hiding CP-ABE*. In ISPEC, pages 24-39, 2011.

[14] *Strategies For regulating electronic Health records exchange*.- NYCLU Report, 2012

[15] S. Narayan, M. Gagn_e, and R. Safavi-Naini. *Privacy preserving EHR system using attribute-based infrastructure*. In Proceedings of the 2010 ACM Cloud Computing Security Workshop, 2010.

[16]Microsoft.*MicrosofHealthVault*,2011. http://www.healthvault.com/personal/index.aspx.

[17] AbuKhousa E, Mohamed N, Al-Jaroodi J (2012) *e-Health Cloud: Opportunities*
and Threats. J. Network and Computer Applications 35: 211-220

[18] *CSCC healthcare-Impact of Cloud Computing on Healthcare*- November 2011.

[19] *United states dept of Health & human services*- HITECH, HITECH Act enforcement intern final Rule, 2011, http:// www.hhs.gov.

[20]*Symmetric key encryption* wikepidea http:// www.symmetrickeyencryption.com

[21] Amit Sahai and Brent Waters, Fuzzy Identity-Based Encryption Cryptology ePrint Archive, Report 2004/086

[22] Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters, Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data ACM CCS (2006).

[23]Adi Shamir , ID-based Cryptosystems and signature schemes Advances in Cryptology: Proceedings of CRYPTO 84, Lecture Notes in Computer Science, 7:47--53, 1984 .