Security of PHR Model on Public Cloud using MultiAuthority and Key Policy Attribute based Encryption

Pooja K. Patil
Department of Information Technology, STES's Smt. Kashibai Navale College of Engineering, Pune, India

P. M. Pawar
Department of Information Technology, STES's Smt. Kashibai Navale College of Engineering, Pune, India

ABSTRACT
Personal Health Record (PHR) is a web based set of tools that provides the facility to exchange and maintain a complete electronic health record of a patient. Third-party service providers are available to maintain PHRs like HealthVault1, Google Health or Web MD. These applications allow individuals to enter, store and share their own health data, upload health measurements from their devices or from hospital EHR systems. Another alternative is to outsource PHR to the third party cloud service providers or on semi trusted servers. It helps to increase PHR efficiency and to overcome problems associated with maintaining own specialized data centers. However, serious privacy concern arises as data are exposed to unauthorized users. The potential solution to this problem is to encrypt the data before outsourcing, however while encrypting data the issue of key management, data privacy and fine grained access remains a major concern. Taking these issues into consideration the paper proposes a model for securing PHR stored in semi-trusted third party servers by adopting attribute-based encryption (ABE). The advantage of ABE is, the complexity of encryption and decryption linearly increases with the increase number of attributes which are desired for large systems, although the challenge to make system collusion resistant need to be handled efficiently. To overcome these challenges the model proposes the use of dual system encryption methodology. The encryption techniques from Multi-authority ABE and Key-Policy ABE are combined. Use of MA-ABE technique proves beneficial for key management and flexible access and potential security threat of colluding users is handled by KP-ABE. To this end, proposed framework has attempted to achieve data security by MA-ABE and data privacy by KP-ABE scheme thus improving overall security of the system.

Keywords
Attribute based encryption, Attribute Authority cloud computing, MA-ABE, KP-ABE, data security, fine-grained access control, Personal Health Record.

1. INTRODUCTION
The current environment encourages the growth of digital media for storing and sharing health information.PHRs are mainly used by patients, healthcare providers, policy makers, insurance companies and families.Although, the cloud platform seems to be viable for PHR systems , data security still remains a major impediment in its wider adoption. This then also warrants the need for stronger encryption techniques that work with semi-trusted servers.

To address these issues the use of attribute-based encryption (ABE) as the core encryption technique is proposed .In ABE access policies are articulated on the attributes of users or data which eliminates the need to know an Access Control Lists (ACLs) .A PHR should only be available to set of users with the alternative decryption key without exposure to rest users. The patient retains the rights to grant as well as revoke the access privileges [1].Considering these all factors the proposed framework has the following key features:
1.The framework focuses on patient centric and secure sharing of PHR records in a multiowner environment on a semi trusted server. The system is divided into *public* and *personal* domains e.g. family members and friends in personal domain, similarly medical doctors, pharmacists and researchers in the public domain. This type of arrangement helps in easy key management .In addition framework also supports write access control, runtime policy updates and competent handling of emergency cases.

2. In the public domain multi-authority ABE (MA-ABE) is used .The concept of Attribute Authority (AA) is originated from MA-ABE [2]. Each AA controls the different subset of user role attributes; hence no single authority is responsible for maintaining the security of the whole system. In the personal domain, an owner is able to provide access rights to the users to encrypt PHR file under its data attributes. The arrangement helps in resolving the traditional key management problems for large systems.

3. Proposed framework also aims to use central Authority (CA) along with attribute authority. Although CA will validate the users in the system he is not accountable for management of attributes. The idea of distributing the load of generation of secret key on different AA and not on single CA will promise the system security as long as some of AAs are honest.

Contribution of this paper:
In MA-BE scheme if user A has the key associated with the access structure “X AND Y”, and User B has the key associated with the access structure “Y AND Z” users will be able to decrypt a cipher text whose only attribute is Y by colluding. Hence proposed model uses two level random masking methodologies MA-ABE and KP-ABE. Primarily information is encrypted using the MA-ABE and private key is generated by the contribution of each attribute authority. Encryption technique KP-ABE is used to generate an attribute key which is completely based upon the access structure of attributes of individual authority and it is time varying. Hence, even if the authorities collude, data security can be achieved with the help of attribute key.

This arrangement makes the system highly secure against unforeseen cases i.e. even if N − 2 AAs (where N represents the total number of AAs in the system) are compromised [3].

1.1 Organization

The remainder of this paper is organized as follows: Section II provides the related work with an overview of existing ABE Schemes Section III presents the assumptions and the system model considered in proposing PHR framework. Section IV provides the detail overview of the MA-ABE and KPABE scheme, Section V details the system architecture. Further results are presented and discussed in section VI and section VII concludes the paper.

2. RELATED WORK

ABE has been used and mentioned in various works to realize fine-grained access control of outsourced data [4]. A basic property of ABE prevents against user collusion, also encryptor need not worry about ACL.ABE is widely applied to secure electronic health records(EHRs)[5].Recently Narayan et al. proposed an attribute based system for EHR systems .The variants of attribute encryption techniques used for fine grained encryption of data are explained below. In [8] Bethencourt and Sahai used a ABE variant where delegation of access rights is proposed for encrypting EHRs.In [6][7], Akinyele et al. generated EMRs, which can either be stored on cloud servers or on mobile devices with the help of ABE. This proves useful, as EMR could be accessed when the health provider is offline. However the drawback is that the authors usually assume a single trusted authority and central Authority. First arrangement gives rise to serious key escrow problems while a second is prone to major security threat.Finally, most of the existing literature does not set apart personal and public domains, which are subject to diverse attribute definitions, key organization requirements and scalability issues. Idea of conceptually dividing the system in two types of domains is similar to that in [8], however a key difference is that in [8] a single TA is still assumed to be an administrator in the professional domain which can again be an security threat.

3. ASSUMPTIONS AND PROPOSED FRAMEWORK

3.1 Problem Definition

To provide a secure framework for patient centric sharing of PHRs in a multiple authority and a domain PHR system with several users using the MA-ABE and KP-ABE schemes. It is proposed that a central server is to be managed by a third party service provider to store all PHR The User is supposed to access the PHR in order to read or write as well as access the data from multiple data owners.

3.2 Security Model

The server in consideration is a semi-trusted, i.e. truthful but interested as in [9] .It implies that servers will attempt to dig most secret information in PHRS, but will follow the set of rules in general. For example a researcher may try to access any personal information of patient other than the beneficiary information of his use. For this the researcher may collude with other users or even with the server. Further it is assumed that the PHR system consists of public/private key pair and user authentication can be done by conventional challenge-response protocols.

3.3 Requirements

The security and performance requirements are detailed as follows:

Data Privacy: No unauthorized user including server will be able to decrypt the PHR if they do not posses satisfying access policies.

On-demand revocation*:* If the time period assigned for accessing the attributes expires then no user will be able to access the PHR files using that attribute.

Scalability and efficiency*:* PHR system will support the increasing numbers of users from public domain and personal domains. Eventually the framework will be able to handle the key management with increased number of users. Further the difficulty experienced by attribute authority in controlling the users and keys will be minimized.

3.4 Framework Details

The key idea is to segregate the system into multiple security domains i.e. (public domains (PUDs) and personal domains (PSDs) in line with the data access requirements of different user's [4]. The PUDs consist of users who can access the system based on their specialized roles, such as medical practitioners, medical researchers and nurses. Conventionally a PUD can be looked as an autonomous sector such as the health care, government or insurance. For each PSD, users are individually associated with a data owner (such as relatives or near friends) and they access PHRs based on rights given by the owner.

In PUD multi-authority ABE is used along with KP-ABE. Users in the public domain obtain their attribute-based secret keys from the AAs, without contacting the owners. Since the PUDs contain the majority of users, it reduces the key management overhead for both the owners and the users; furthermore it also solves the key escrow problem related to single trusted authority. In PSD KP-ABE scheme is adopted as data owner (i.e. patient) is the trusted authority of PSD he/she will be responsible for generating secret keys and granting access rights to users. In PSD burden on the owner is not much as numbers of users in a PSD are often less.

The multidomain approach best fits the PHR system because multiple user types and their different access requirement are handled efficiently. The use of the basic ABE and MA-ABE and KP-ABE scheme guarantees the access to data only by authorized users and enhanced security. Both these schemes are explained in more detail as below.

3.4.1 Multi-Authority ABE

The majority of the previous work on data security considers attributes to be governed by single authority However from a security viewpoint, dividing it into multiple authorities is a more feasible solution. The vital challenge is to prevent the system from two colluding users, users may pool their keys to decrypt a message that they are not entitled to **.**The proposal suggested by [9] is similar to one proposed by this work, i.e. it does not rely on the central authority. However the scheme suggested by [9] guarantees *M-resilience* in the security that is against a maximum of m colluding users However this notation of security is undesirable for large systems with multiple users as proposed in this work. With increasing number of users in the system, the risk associated with the number of users being compromised will also increase. Hence this work argues that it a open problem to design a competent and secure multi-authority ABE scheme without a trusted CA and attempt has been made to solve it. The MA-ABE scheme is implemented as follows and consists of seven algorithms

- **Setup:** The setup algorithm takes no input other than the implicit security parameter. It generates the public parameters PK and a master/secret key MK generated by each AAs.The N-th AA defines a disjoint set of role attributes U*r*, which are fairly common for public users. As these attributes are classified on the basis of their profession.
- **Key Generation (MK, SK):** The key generation algorithm uses the master key MK and a set of attributes U*r* that describe the key, and outputs a secret key SK for user U. SK should contain at least one attribute from every type of attributes governed by AA.
- **Encryption (PK, M,** U*r***):** The encryption algorithm takes as input the public parameters PK, a message, M and an access structure A over a set of attributes Ur. It will encrypt M, and produce a cipher text CT such that only a user who possesses the set of attributes satisfying the access structure will be able to decrypt CT.
- **Decryption (PK, CT, SK):** The decryption algorithm takes as input PK, a cipher text CT, which was obtained for set of attributes Ur, and a private key SK for Ur. If Ur satisfies the access structure A, then the algorithm will decrypt the cipher text and return a message M.
- **Create User (PK, MK, U):** The Create User algorithm takes as input the public key PK, the master key MK, and a user name U. It outputs a public user key for user i.e. PK, .This key will be used by AA to issue secret keys for user U .The secret user key SK, can be used for the decryption of cipher texts.
- **Create Authority** (PK, *a*):The *Create Authority* algorithm is executed by the admin with identifier *a* once during initialization. It outputs a secret authority key SK*a* for the attribute authority.
- **RequestAttributeSK** (PK, *A,* SK, U)**:** The Request Attribute SK algorithm is executed by the attribute authority whenever it gets a request for a secret attribute key. The algorithm verifies whether the user U with public key PK is eligible for set of role attributes. If the condition satisfies *Request Attribute* outputs a secret key SK for the user U is the algorithm returns Null value

3.4.2 Key Policy Attribute-Based Encryption (KP-ABE)

In KP-ABE secret key is associated with the access structure in contrast to MA-ABE where the secret key is associated with attribute authorities. In this work same concept has been used i.e. MA-ABE is to be used for data encryption and to obtain the secret key on attribute authority basis. It is assumed that some of the authorities may be corrupt and hence an *attribute key* is to be generated based on KP-ABE scheme. The model will encrypt the access structure P1 for e.g. *P*1 : =" (*Profession=Doctor*)∧ (*specialty=cardiologist Medicine*) ∧ (*organization=hospital X*) ∧ *Licenses = IMA)*". By decrypting the access structure an attribute key will be generated which will also be a secret key and will be different for each user based on access to different attributes. In this system even if the users collude the attribute key will be different for each authority providing two levels of security. A (Key-Policy) Attribute Based Encryption scheme consists of four algorithms as follows:

3.4.3 Definition Access Structure

Let {P1..... Pn} be a set of attributes. A collection A $\subseteq$ {P1..... Pn}is monotone If $\forall$ B,C: if B $\subseteq$ A and B $\subseteq$ C, then C $\subseteq$ A . An access structure is a collection A of non-empty subsets of {P1, Pn} i.e., A $\subseteq$ {P1 ... Pn} \{}. The sets in A are called the authorized sets while those sets not in A are called the unauthorized sets.

- **Setup**: This is a randomized algorithm that takes a security parameter as an only input. It generates the public parameters PK and a master key MK. Here master key is also referred to as Attribute Key.
- **Encryption**: This is a randomized algorithm that takes as input - a access structure A i.e. a set of attributes, and the public parameters PK. The output is cipher text E
- **Key Generation**: This is a randomized algorithm that takes as input - an access structure A, the master key MK and the public parameters PK. The output here is a decryption key or Attribute Key AK
- **Decryption:** This algorithm takes as input - the cipher text E that was encrypted under access structure A, the decryption key AK and the public key PK. The output is message M.

As above, this work presents the dual technique of encryption. In the encryptor's dual access policy the former one is across *different attribute authorities (MA-ABE)* and lateral is across *different attributes* governed by the same AA (KP-ABE).The proposed system addresses the most important issue of data security in addition to efficient attribute revocation and fine grained data access.

4. SYSTEM ARCHITECTURE

In the proposed system, PHRs are stored in the semi trusted cloud and can be accessed through web application by multiple owners and users. The owner of this system is considered to be an administrator and is responsible for creating access policies based on the professional role of the user. PHR data are stored in the cloud in an encrypted format. Two cloud or web services have been designed. The first web service is accessible to the user and is used for hosting web portal, generating access policies and for other computing tasks. The second service is used for encryption/decryption logic and is accessed by first web service; the majority of the computational task is delegated to Cloud Servers. Figure 1 shows architecture for the proposed cloud based PHR system. The combination of RSA, AES and DES are used as the encryption algorithm, based on the attribute nature. It helps to reduce the encryption /decryption time.

5. SECURITY ANALYSIS

Cryptographic technology is mature and well proven and can prevent from outside attacks as well as penetration within the organization itself[10].Therefore attacks like eavesdropping, Man-In-The-Middle, and Denial-of-Service (DoS) are handled efficiently by encrypting the data. In proposed model phr files are encrypted by AA and decrypted by users using two level encryption technique, thereby performing all end to end operations. This ensures that the data confidentiality and integrity is not compromised. All users and authorities in the system are registered with the CA as well attribute authority also perform authorisation before granting access rights to any attributes this arrangement helps to resists MITM attacks. There are other techniques also, through which phr application is made secure. DBA does not have access to encryption keys or the services that can decrypt data. The encryption keys can only be decrypted by the security process. Secondly, the encryption keys and data are securely stored in different databases. It helps to restrict complete access to the database by unauthorized user. Further, the combined use of

RSA, AES and DES algorithms for the same data enhances the security of data, as intruder cannot find the encryption pattern easily. All these security majors help to prevent the data from external attack.

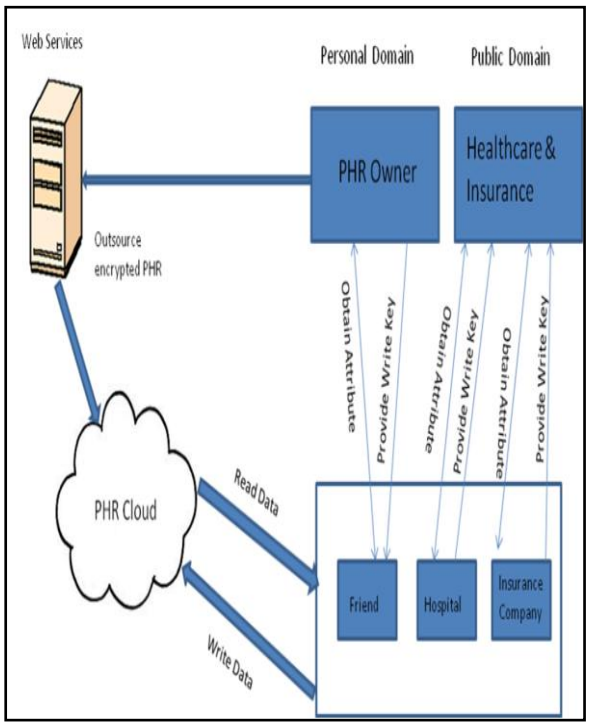

Fig 1: Proposed system model for ABE –PHR system

In next section, the internal security of phr model is analyzed in terms of data confidentiality and collusion resistance.

5.1 Data confidentiality

In [4],[5] the original MA-ABE scheme has been confirmed secure under the attribute based selectors-set model given the Decisional Bilinear Diffie-Hellman (DBDH) problem is hard. Which means a user who does not clutch sufficient access privileges that satisfy the data attributes of a PHR file cannot decrypt the file. For MA-ABE as it is used in the same way as CP-ABE, security analysis should be a user who does not have a set of role attributes that satisfy the PHR file's access policy cannot decrypt the PHR file.

In proposed system the enhanced version of the MA-ABE and KP-ABE is used to encrypt each PHR file .The composition of both schemes is more secure as they are self sufficient cryptosystems with separate attribute universe and private /public keys.

5.2 Collusion Resistance

In [5] framework is similar to proposed solution i.e. using the MA-ABE and is made collusion resistant among N-2 AAs (N is the total number of attribute authorities in the system). The scheme uses the dummy attribute which is compulsorily ANDed with original access policy. Hence, if numbers of users and access policies go on increasing the computational overhead will also increase. Secondly, the cost of this solution is prolonged public keys, user secret keys and cipher texts (extended with additional N −2 components). The deception of N-2 AAs implies that the scheme can be compromised with last two AAs getting compromised. Proposed framework can handle this extreme case, i.e. even if all AAs are compromised then also PHR security can be achieved with the help of attribute key based on KP-ABE .This is derived from the fact that every user will have different attributes key based upon attribute set. The point to be considered is that attribute set will always vary, depending upon professional requirements, time period and also for some additional attributes user request in the system from other AA. Hence, there are very little chances that attribute key will be same for any two users for a given period of time.

5.3 Performance Analysis

The performance analysis is done as follows. Proposed study is compared with a solution that of [15] which uses KP-ABE, and a single public authority in the number of PUDs, while Ni is the number of AAs in the ith PUD. The key management complexity is in terms of the number of interactions during key distribution. $\mathbb{A}_k^C$ Attributes in the cipher text (from the kth AA). Ciphertext length comparison, for proposed scheme is based on the access policy for each PUD and is restricted to conjunctive form: P : = P1 ∧ ..... ∧ Pi, where each Pi is a Boolean clause consisting of "∧ "and "∨ ". Number of cipher text components related to the PUDs is

$$|\mathbb{A}^c| = \sum_{j=1}^{m} (\sum_{k=1}^{N_i} |\mathbb{A}_{k,i}^C|)$$

This is linear to the number of PUDs and the number of AAs. In practice, there are usually a few PUDs (e.g., < 5) and a few AAs and types of attributes in each of them (e.g., 5). Therefore the additional storage overhead for the server created by each ciphertext (encryption of the file with an encryption key) is usually in the order of tens of group elements, which typically equals to a few hundred bytes. This is acceptable compared with the length of a PHR document (usually in the order of KB). Apart from those, for each owner, to change access policies and enable emergency access, two additional group elements (s and d) shall be locally stored for each encrypted PHR file, which is quite small. Finally, the computational overhead in proposed scheme is low, since the decryption operation can be mostly delegated to the server.

6. RESULTS

6.1 Key Generation Time

The key generation time required for existing and proposed KP-ABE scheme is shown in Fig 3. The time required by proposed KP-ABE scheme is slightly less than the existing scheme. As the proposed scheme encrypts the access structure by finding out ASCII value of each character in access structure. The access structure consists of attributes with boolean formula of "AND, OR". The traditional method of encrypting an access structure by some known public/private key algorithms introduces the overhead of public/private key. The secret key which are generated by these algorithms also deal with the overhead of key distribution.

The complete time required in key generation i.e. secret key and attributes key using dual encryption technique verses the time required in the generation of Secret Key by KP-ABE and MA-ABE is shown in Fig 2 . The encryption/decryption time and key generation time linearly increase with increase in number of attributes. The time required for key generation in KP-ABE is comparatively less than the CC-MAABE as existing CC MAABE scheme uses additional dummy attributes in the access structure which results in prolonged

public keys and user secret keys which also means increased key generation time. Proposed scheme requires almost the same time for key generation or slightly less as compared to CC MAABE because in proposed scheme use of dummy attribute is not done; hence the secret key size is not increased. The attribute key is generated by efficient KP-ABE scheme which also takes less time (as shown in fig 3). Hence the dual encryption arrangement takes approximately same (or slightly more) key generation time but achieves more security.

6.2 Encryption/Decryption Time

The encryption and decryption time required for the MA-ABE, KP-ABE and combination of both i.e. proposed scheme is shown in Fig 4 & 5. Proposed scheme shows a minor increase in the encryption and decryption time. This is because of nature of dual encryption techniques followed.

6.3 Security Analysis against colluding users

For security analysis three representative state-of the- art schemes are used to compare with: 1) the VFJPS scheme based on access control list (ACL) 2) The RNS scheme in that enhances the Lewko-Waters MA-ABE with revocation capability for data access control in the cloud 3.)Existing enhanced MA-ABE scheme. The VFJPS scheme requires each owner to publish a directed acyclic graph representing her ACL along with key assignments, which essentially amounts to complexity of O(Nu) per owner where N are total authorities in the system. This puts a large burden either in communication or storage cost on the system.VFJPS scheme do not have security against user-server collusion. In RNS the AAs are independent with each other, while in proposed scheme the AAs issue user secret keys collectively and interactively. Also, the RNS scheme supports arbitrary monotonic Boolean formula as file access policy and revocation. However, in proposed scheme user revocation method is more efficient in terms of communication overhead. In RNS, upon each revocation event, the data owner needs to recomputed and send new cipher text components corresponding to revoke attributes to all the remaining users. In the proposed scheme, such interaction is not needed. RNS has revocation means that are at the Attribute - level have immediate and has security against N-1 AA collusion. In enhanced MA-ABE scheme secret key updates are delegated to the server, a dummy attribute needs to be additionally defined by each of N −1 AAs, which are always ANDed with each user's key-policy to prevent the server from grasping the secret keys. This also maintains the resistance against N −2 AA collusion attacks. Proposed MA-ABE can resist collusion attack even though all N authorities in the system collude with each other. Fig 6 shows the security analysis for VFJPS, RNS, existing MA-ABE and proposed MA-ABE. The Y-axis consists of security against no. of colluding users. I. e out of n users in the system , if one or two users get compromised then system is prone to collusion attack.

7. CONCLUSION

The proposed paper discusses platform for sharing of personal health records in the secure and scalable manner by using semi trusted cloud. As cloud considered here is moderately trustworthy patient data privacy is guarded by encrypting the data before outsourcing.

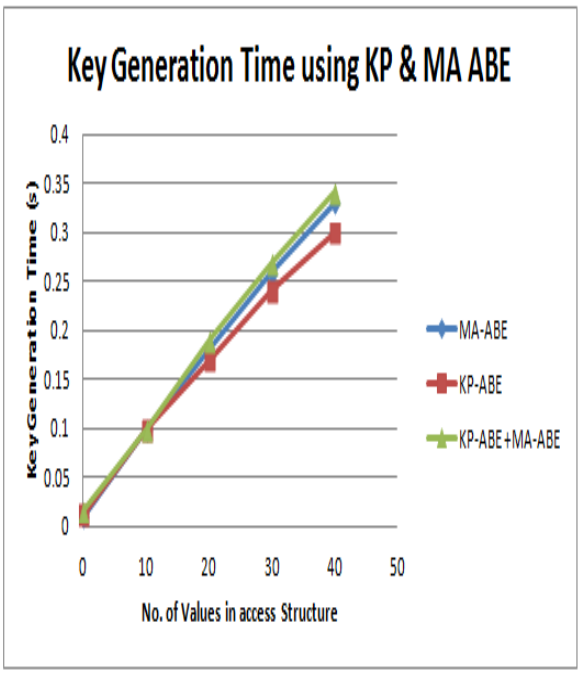

Fig 2. Key generation graph using both encryption techniques

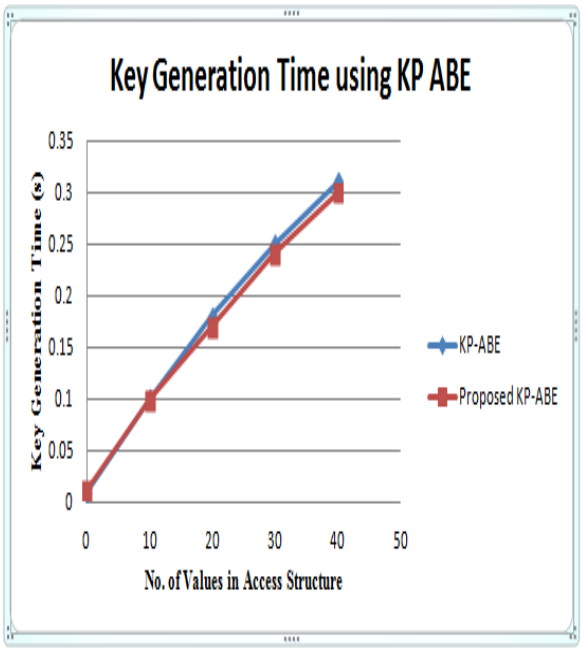

Fig 3. Key generation time for KP-ABE schemes

The multi domain approach suits the practical scenario in PHR management and simultaneously helps in reducing the complexity in key management. Further an attempt is made to increase the security of the system by combining two encryption techniques. It is noted that using ABE and MA-ABE improves system scalability but there are some practical limitations in the building PHR system. For example in workflow depending access scenarios, data admittance right is based on users' identities instead on their attributes and ABE schemes cannot handle this competently. In such cases one may think of using attribute-based broadcast encryption [11]

or distributed ABE schemes. This issues may be delegated as future works.

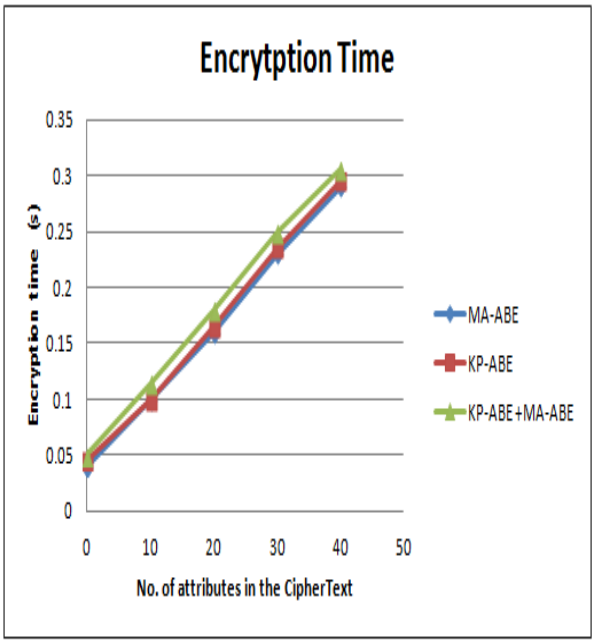

Fig 4. Encryption time

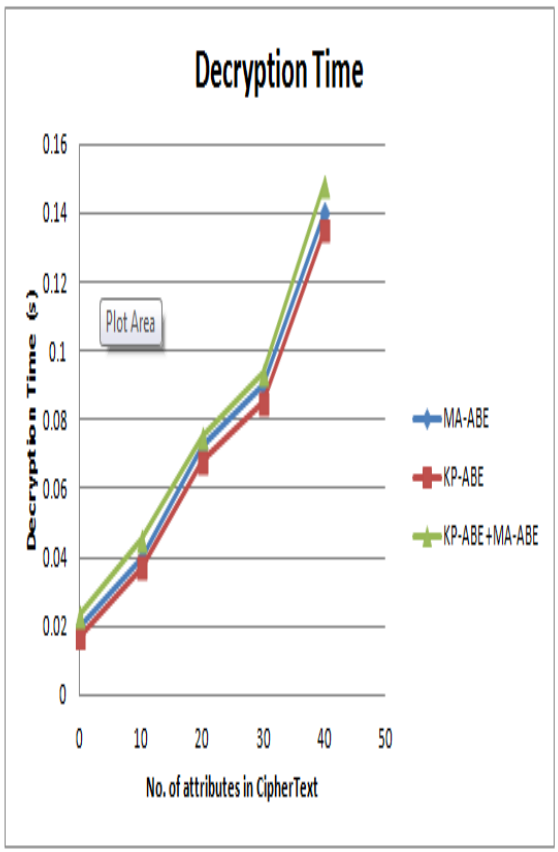

Fig 5. Decryption time

-

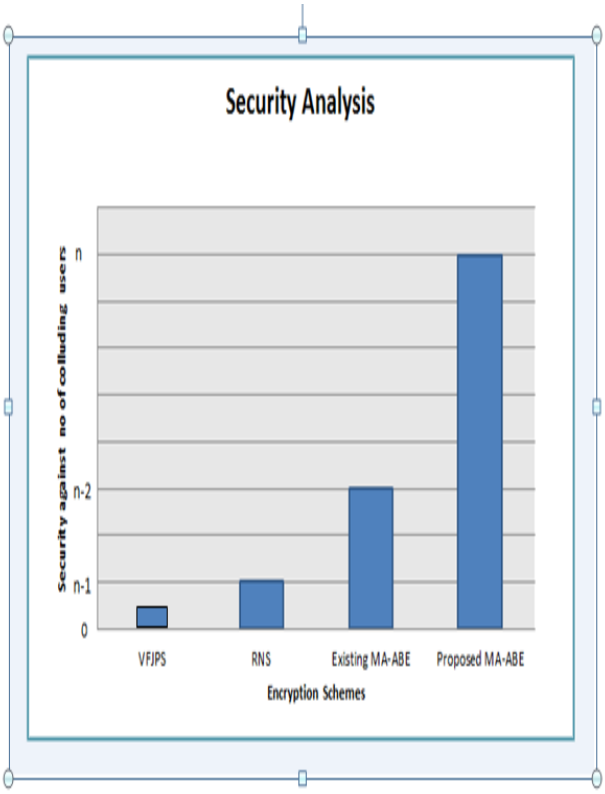

Fig 6. Security analysis against colluding users

7. REFERENCES

[1] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records,"in CCSW ,Nov 13, pp. 103–114,2009.

[2] Ming Li., Shucheng Yu, Yao Zheng, Kui Ren, Lou" Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption" IEEE transactions on parallel and distributed systems,vol.xx,no.xx,2012

[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in IEEE INFOCOM'10,May 12-15,pp.73, 2010.

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters,"Attribute-based encryption for fine-grained access control of encrypted data," in CCS '06, October 30–November3,pp.89–98,2006.

[5] 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, no. 7281, p. 283, Feb. 2001.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in IEEE S& P '07, Sept 7, pp. 321–334,2007.

[7] J. A. Akinyele, A. Sahai ,C. U. Lehmann, M. D. Green, M. W. Pagano,Z. N. J. Peterson, and A. D. Rubin, "Self-protecting electronic medical records using attribute-based encryption," Cryptology ePrint Archive, Report

2010/565, 2010, http://eprint.iacr.org/

[8] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Patient self-controllable access policy on phi in ehealthcare systems," in AHIC'10,vol.6,Dec 7 ,pp1-5 ,2010.

[9] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in CCS '09, BMJ. 25, pp.121–130,2009.

[10] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 99, no. 7,July ,PrePrints, 2010.

[11] N. Attrapadung and H. Imai, "Conjunctive broadcast and attribute-based encryption," Pairing-Based Cryptograph ,in ASIACCS'10,Vol.40,No.26, pp. 248–265, 2009