**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

***IJCSMC, Vol. 4, Issue. 12, December 2015, pg.324 – 329***

# Secure Patient Health Record Manager Using Attribute-Based Encryption

**Ms. Reshma S. Sapakal[1], Mr. Pankaj R. Chandre[2]**

[1][2]Department of Computer Engineering, FIT Pune, Pune University, Maharashtra, India

[1] reshma.sapakal86@gmail.com; [2] pankajchandre30@gmail.com

***Abstract— Patient health record manager (PHRM) is system of health information management under the control of patient and data is stored at a third party, such as cloud service providers. This system must provide wide privacy to patient health information while it exposed to those third party servers and to unauthorized users. To assure the patients' control over access to their own PHRMs, system must encrypt their information before outsourcing. Then also there is risks of privacy, scalable key management, flexible access and user revocation to be done efficiently are some remained the vital issues while achieving secure access. Using cryptography data access can be controlled. In this paper, we propose a system which is controlled by a patients and mechanisms for data access control to PHRMs stored in third party servers. In PHRMs for achieving smooth and scalable data access control, attribute based encryption (ABE) techniques is used to encrypt each patient's PHRM file. While providing secure data outsourcing, the main concentration is the multiple owners of data, and divides the users in the PHRM system into multiple security domains. Because of this system greatly reduces the key management complexity for data owners and users. PHRM guaranteed high degree of patient privacy.***

***Keywords— Patient health record management, cloud computing, data privacy, fine-grained access control, attribute-based encryption***

## I. INTRODUCTION

The Internet has grown very fastly in recent years and is offers various capabilities that could support Physicians to do their duties in numerous ways. With the development of information and medical technology, medical information has been transformed from traditional paper records into electronic medical records which are widely used. Nowadays software systems have evolved from the individual user's local hardware to a central server that operates from a remote location. A health record is nothing but record of an individual user's health information stored in computer and user has the individual controls access to the information and have the ability to manage, track, and participate in own health care.. According to a recent report [1], there are more than 77% patients and 70% physicians want to involve in mHealth systems by using their own mobile devices. The

 

important issue is whether the patients actually control the sharing of their sensitive personal health information (PHI). Particularly when patients store their information on a third-party server which is not fully trusted by people? While storing the ePHI (Electronics Personal Health Information) user need to guaranteed integrity, confidentiality and availability of information. They also assure protection against possible vulnerabilities to the privacy of the information.building and maintaining specialized data centers is very costly so many medical record services are stored on third-party service providers like CSP , for example, Samedi, Microsoft HealthVault and Medicine Brain.

### *A. Motivation*

Patient Health Records contains- Patient's regular Information, Medical details and past if any, Examination Reports, Insurance Information, and Sensitive Information. Several medical records can face theft and stolen incidents [2], in which attackers can steal and publish patient health information to a third party or over the Internet. According to a recent survey, researchers spent 41.3 billion dollars per annum to estimate the economic impact of medical identity theft in the United States .More than 78% of participants [3] concern about the leakage and abuse of their personal information and health condition. So users fear to use eHealth/mHealth systems. For most eHealth/mHealth [4] systems, physicians periodically upload their observations to a particular storage. A secure feasible and promising approach is to use encryption techniques for the data before outsourcing on third party server for providing security and privacy. Here the PHR owner will decide how to encrypt the files and to allow which set of users has authority to access each file. The patient has full right to grant as well as revoke access privileges from user when they feel it is necessary [7].Also in existing systems there is the single data owner scenario [8], [4]. ButPHRM system provides multiple owners scenario where owners can encrypt according to their wish. Multiple ownersuse different sets of cryptographic keys for encryption. The attribute-based encryption [12] (ABE) algorithm can be a good solution to those problems and to easily outsource the PHRMs as in Chase and Chow [10].

## II. LITERATURE SURVEY

For access control of the data outsourced, partially trusted servers are used. Using cryptosystem, security can be provided to outsourced data. With cryptographic methods, the aim is trying to enforce who can (read) access to which parts of a patient's PHRM documents in a fine-grained way. For security purpose different encryption methods can be used like Symmetric and Public Key Encryption, and Attribute Based Encryption. Attribute-based encryption (ABE) is a new approach that reuses the public-key cryptography concepts. In public-key cryptanalysis a message is encrypted using the public key shared by receiver. New identity-based cryptography changes the traditional concept of public-key cryptography. It allows the public-key to be an arbitrary string, e.g., the email address or phone no. of the receiver. ABE goes one step further and defines the identity as set of attributes not limited to single atomic key. There are different versions of ABE as MA-ABE (Multi-authority ABE),KP-ABE (key-policy ABE) and CP-ABE (Cipher-text efficient access control, the public key encryption (PKE) [11], [12] can be used. But there is high overhead of key management and require to encrypt multiple copies of a file using different users' keys. To provide the secure and scalable solutions, one-to-many encryption methods like ABE can be used. In Goyal et al.'s seminar paper on ABE [13], data is encrypted using attributes set so that multiple users can decrypt it. This makes encryption and key management more efficient [12]. KP-ABE (key policy attribute-based encryption) algorithm used for access control scheme for PHRMs [6]. Using KP-ABE the efficiency and security of the scheme could not be guaranteed. But because the data owner also was the TA (rusted Authority) and the program didn't changes the random parameter of ABE there is efficiency problem. To solve the efficiency problem of KP-ABE a MA-ABE access control strategy under cloud storage is used.

## III. EXISTING SYSTEMS

Many PHRM-related research opportunities exist in the market for individuals and organizations studying sociotechnical issues. The cost of building and maintaining specialized data centres is very high; so many PHRM systems are outsourced to third-party service providers. E.g. Microsoft Health Vault. It will be very exciting to have convenient PHRM services for everyone but there are many security and privacy risks. The main issue is whether the patients actually control the sharing of their sensitive patient health information (PHI).Particularly when they are stored on a third-party server which people may not fully trust? The disadvantages of existing systems are found as following example. The department of Veterans Affairs database containing sensitive PHI of 26.5 million military veterans. This PHI includes their social security numbers and health problems. This PHI was stolen by an employee who took the data home without authorization. They assume single trusted authority (TA) in the system is safe. This not only may create a load bottleneck, but also face the key written agreement problem as the TA can access all the encrypted files, opening the door for potential privacy exposure.

 

## IV. PROPOSED SYSTEM

We consider a PHRM system where there are multiple PHRM owners and users. The owners are nothing but patients having full control over their own PHRM data, i.e., they can create, manage, and delete it. There is a central server belonging to the PHRM service provider that stores all the owners' PHRMs. The users may be a friend, a caregiver or a researcher. Users access the PHRM documents through the server in order to read or write to someone's PHRM, and a user can simultaneously access multiple owners' data. A typical PHRM system uses standard data formats. The main goal of this framework is to provide secure and efficient PHRM access controlled by patient and efficient key management at the same time.

To provide interoperability, PHRM support the same communications, messaging, and encoding standards. Because the public and medical professionals use PHRMs, we have to develop "lay" representations and explanations of the encoded data. There are authentication vexing problem for PHRMs. A stand-alone PHRM device may be safe if it is constantly under the control of the owner. But what happen when its contents are unencrypted and the device is lost in a public area? And as the PHRM interact with other health care system, authentication becomes very important. Before another health information system shares data with a PHRM, it will need to verify the identity of the PHRM's owner.

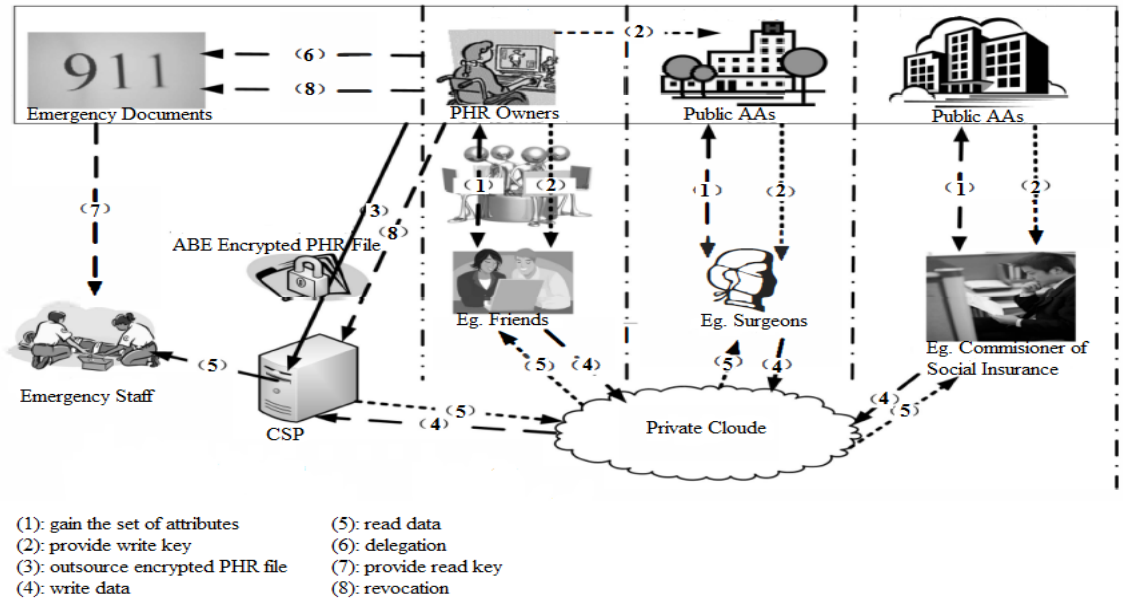


Fig 1 The framework for PHRM access control under multi-owner settings

As shown in the Fig 1, the owners upload encrypted PHR files using ABE to the server ((3)). Each owner's PHR file is encrypted and role-based access policy assign to users from the PUD for accessing purpose. Under a selected set of data attributes is accessed by the users in the PSD. The data readers download PHR files from the server and can decrypt the files only if they have suitable attribute based keys ((5)). The write access can be granted to user of PHRM, if they present proper write keys ((4)).

### *A. User Revocation*

For revocation of a data reader or their attributes/access privileges following are possible cases: 1) revocation of one or more main attributes of user of a public domain; 2) revocation of a public domain user which is same as to revoking all attributes of that user. These operations are done by the AA to which user belongs, where the actual computations can be send to the server to improve efficiency ((8)). 3) Revocation of a PSD user's access privileges; 4) revocation of a PSD user. These can be initiated through the PHR owner's client application in a similar way.

### *B. Policy Updates*

A PHR owner can update her sharing policy by updating the attributes (or access policy) in the ciphertext. The supported operations include add/delete/modify, which can be done by the server on behalf of the user.

 

### *C. Break-glass*

When an emergency happens, the regular access policies may not be applicable here. To handle this situation, break-glass access is needed to access the victim's PHR. In the framework, each owner's PHR's access right is also delegated to an emergency department (ED), (6)). To prevent from misuse of break-glass option, the emergency staff needs to contact the ED to verify her identity and the emergency situation, and obtain temporary read keys ((7)). After the emergency is over, the patient can revoke the emergent access via the ED.

## V. ALGORITHMS

### *A. Introduction*

An encryption algorithms are important for securing the data while storing or transferring it. The encryption algorithms are classify as Symmetric (secret) and Asymmetric (public) keys encryption.
In Symmetric key encryption, only one key is used for both encryption and decryption of data. Eg: Data encryption standard(DES), Triple DES,
Advanced Encryption Standard(AES) and Blowfish Encryption Algorithm

In asymmetric key encryption or public key encryption[1] uses two keys, one for encryption and other for decryption. Eg: RSA

### *B. Blowfish Encryption Algorithm[2]*

Blowfish Encryption Algorithm was developed by Bruce Scheier in 1993. It is fast and alternative to existing encryption algorithms like AES, DES. Blowfish is a symmetric block encryption algorithm. It encrypts data using 32-bit microprocessors with rate 26 clock cycles per byte This speed s considered fast.
Compact: It use less than 5K memory to run.
Simple: It uses XOR, addition, lookup table with 32-bit operands for encryption.
Secure: The key length is variable. it can be in the range of 32~448 and bits: default 128 bits key length. This algorithm is suitable for applications where the key does not change frequently.

The Feistel structure of Blowfish

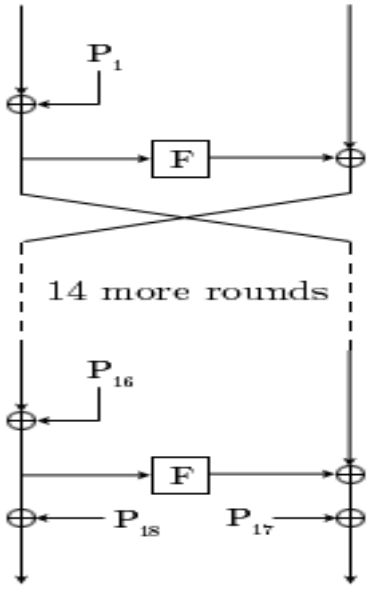


Fig 2: The Feistel structure of Blowfish

*1) Description of Algorithm:*

Blowfish encryption algorithm encrypts block data of 64-bits at a time. It uses the feistel network. This algorithm is divided into two parts.
1. Key-expansion
2. Data Encryption

 

The p-array consists of 18 subkeys of 32-bit each:
P1, P2,……., P18.
Four 32-bit S-Boxes. Each S-Box contains of 256 entries each:
S1,0, S1,1,……. S1,255
S2,0, S2,1,…….. S2,255
……..

XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key. Repeat this cycle until the entire P-array has been XORed with key bits. Continue the process, by replacing all P array entries, then all S-boxes in order, with the output of the continuously changing Blowfish algorithm. Total 521 iterations are required to generate all required subkeys. Applications can store the subkeys rather than execute this derivation process multiple times.
Data Encryption:

It is having 16 iterations in the network. Each iteration contains key-dependent permutation and a key & data-dependent substitution. All operations are XORs and additions on 32-bit words.

In ABE, access policies are expressed using the attributes of users or data, these policies enables a patients to share their PHR among a set of users. The sharing is done by encrypting the file under a set of attributes, without knowing a complete list of users.

### *C. Advantages Of Proposed System*

PHRM focus on the multiple data owner scenario. Thus it divide the users in the PHRM system into multiple security domains that greatly reduces the key management complexity for owners and users. This paper remove this gap by providing a security framework which is patient-centric. This framework is shared in a multi-domain, multi-authority PHRM system with many users. The framework captures application level requirements of both public and personal use of a patient's PHRMs, and distributes users' trust to multiple authorities that better reflects reality.

While solving any software problems its difficulty level must be decides. There are three types of classes provided for that as p, NP complete and NP hard. PHRM is " Hybrid cloud approach for secure authorized DE duplication" is of P complete Class. It is a solvable in polynomial time, so all are NP Problem. It is difficult to compute the time complexity in terms of physically clocked time.

The system first defines a set of data attributes shared by every PSD, such as "basic profile", "medical history", "allergies", and "pulse rate". An emergency attribute is also defined for break-glass access. Each PHRM owner's client application generates its corresponding public/master keys. The public keys can be published in an online healthcare social-network (HSN) (which could be part of the PHRM service; e.g., the Indivo system [17]).

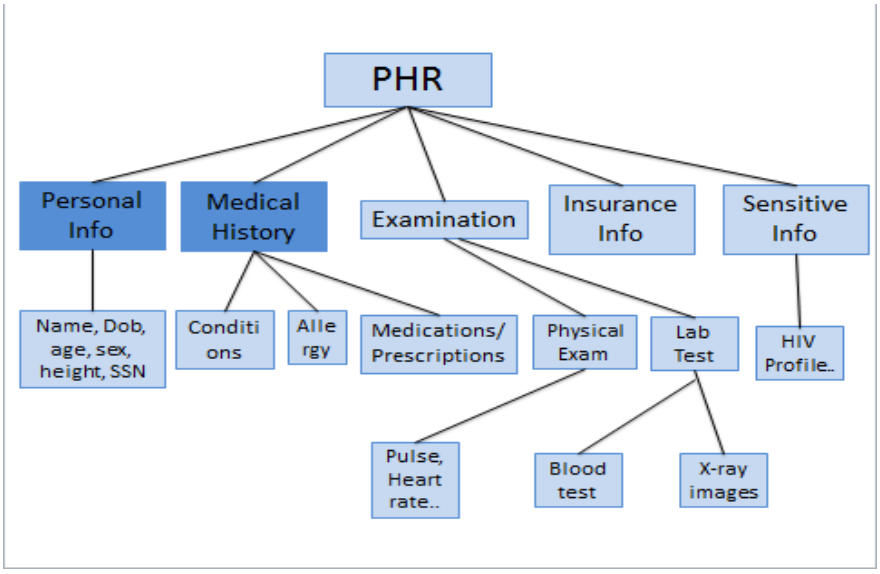


Fig 2.The attribute hierarchy of files

 

### *D. Remarks.*

The separation of PSD or PUD and its data or role attributes shown its reflect in the real-world situation. In the PSD, a patients give personal access of their sensitive PHI to selected users, such as family members and close friends. Second in multi-domain and multi-authority framework, each public user only needs to contact AAs in its own PUD. This AA will generates a secret key for the user, which reduces the workload per AA

## VI. CONCLUSION

Participants describe the plus points of PHRM systems to transform patient–provider relationships. Especially when it is integrated with EHR systems. They also identified many challenges like technical, social, organizational, legal, and financial that must be consider for further study. Users and organizations related to medical field fast adopt PHRMs. Many challenges to deployment of PHRMs are similar to those for EHRs. More PHRM-related research is required. Patients, providers, employers, and other entities which are include in PHRM must play key roles in developing PHRM technology and to overcome the problems of widespread adoption. With a better understanding of the needs and benefits of PHRMs, we can develop better solution. The opportunity costs for PHRM deployment are measured in medical errors, dollars, and lives.

## REFERENCES

[1][Online].Available: http://www.research2guidance.com/us-1.3-billion-the-market-for-mhealth-applications-in-2012/
[2] [Online]. Available: http://www.nytimes.com/2011/11/05/us/ucla-health-system-warns-about-stolen-records.html
[3] [Online]. Available: http://healthcaremgt.net/blog/2011/08/areyou-educating-patients-on-ehr/
[4] LinkeGuo,Chi Zhang,JinyuanSun,Yuguang Fang, "A Privacy-Preserving Attribute-Based Authentication System for Mobile Health Networks" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 9, SEPTEMBER 2014
[5] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: Ensuring privacy of electronic medical records," in *Proc. ACM Workshop CCSW*, New York, NY, USA, 2009, pp. 103–114.
[6] D. Zismer, J. McCullough, and P. Person, "Integrated health care economics. Part 2: Understanding the revenue drivers in fully integrated community health systems," *Physician Exec.*, vol. 35, no. 4, pp. 26–28, 2011
[7] J. Benallie, M. Chase, et al. "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records", CCSW '09 Proceedings of the 2009 ACM workshop on Cloud computing security New York: ACM Press,( 2009).
[8] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes," 2009.
[9] M. Chase, S. S. Chow. "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption", CCS '09 Proceedings of the 16th ACM conference on Computer and communications security, New York: ACM Press,( 2009).
[10] D. Zismer, J. McCullough, and P. Person, "Integrated health care economics. Part 2: Understanding the revenue drivers in fully integrated community health systems," *Physician Exec.*, vol. 35, no. 4, pp. 26–28, 2011.
[11] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in *Proc. SECURECOMM*, Singapore, 2010, pp. 89–106.
[12] J. Jin, G.-J.Ahn, H. Hu, M. J. Covington, and X. Zhang, "Patientcentric authorization framework for sharing electronic health records," in *Proc. 14th SACMAT*, New York, NY, USA, 2009, pp. 125–134.
[13] A. Moumtzoglou and A. Kastania, *E-Health Systems Quality and Reliability: Models and Standards*. Hershey, PA, USA: IGI Global, 2010.
[14] [Online]. Available: http://healthcaremgt.net/blog/2011/08/areyou-educating-patients-on-ehr/
[15] "Indivo." http://indivohealth.org/, 2012.

 