**IJCTA**, 8(4), 2015, pp. 1587-1596
© International Science Press

# Secure and Efficient Data Sharing in Cloud Using Hybrid Patient Controlled Biometric Encryption Scheme

**Rinesh. S.* & M. Mohanapriya****

*Abstract:* Personal Health Record (PHR) is an important tool which used to track the patient information in accurate, reliable and complete manner. The PHR allows the patient to create and update their details and also share their information to other user and health care providers. During the PHR information sharing in the cloud, the users have tackled several problems such as security, scalable key managements, user revocation and flexible access controls. So, this paper proposes an approach Hybrid Patient Controlled Biometric Encryption Scheme (HPCBES) to ensure the security while sharing the PHR into the cloud environment. The HPCBES schemes provide the fine-grained access control to the authorized user with the help of the fingerprint biometric feature. The biometric fingerprint images is linked with the Attribute Based Encryption key and generate the bioscrypt which is used during the verification process and the Multiple Authority Attribute Based Encryption (MAAE) used to grant the access control to the PHR users. The proposed system ensures the security, authentication and efficient data sharing in the cloud environment. The performance evaluation results shows the efficient and secure data sharing with different attribute level of PHR.

*Keywords:* Personal Health Record, Biometric Encryption Scheme, Attribute Based Encryption, Cloud Computing

## 1. INTRODUCTION

Cloud Computing is the emerging technology, which is used to provide the different type of services to the user through the Internet [1]. Cloud system enables the data sharing mechanism which provide the variety of services to the user. According to the Information week survey all the organizations share 74% of their data with customers and 64% of their data to the supplier which is done with the help of the cloud [2]. So, the data sharing place an important role, higher priority and improves productivity in the cloud environment. The shared cloud services are easily accessible via the on-demand network access service and it is flexible which is available at lower cost [3]. During the data sharing the medical data or information sharing plays an essential role because the patient information's are easily accessible with minimum cost.

Now-a-days the Personal Health Record (PHR) is one of the emerging technologies in the medical application which is used to create, manage and update the patient health information in an effective manner [4]. The PHR consist of several information about the particular patient like, identification sheet, problem or significant illness list, medical records, progress notes, consultation details, lab reports, immunization records, consent forms, imaging and x-ray reports and so on [5]. These information records are needed to be stored in the cloud for easy sharing and access mechanism which is used to control the activities of the patients. During the PHR information sharing the fine-grained access control, security, data confidentiality, authorization and authentication is crucial challenge while sharing the PHR records in the third party storage [6]. When the PHR data uploaded in the cloud environment the owner should lose their physical control also it is hacked by some intermediates and internal hackers. So, the security is a major challenge in the PHR data sharing in the cloud environment. The cloud data sharing challenge is

* Research Scholar, Karpagam Academy of Higher Education, Coimbatore, *Email: rineshphd@gmail.com*

** Professor and Head, Department of CSE,Karpagam Academy of Higher Education, Coimbatore.

overcome by applying the encryption approach while sharing the medical information which improves the data confidentiality and data security in the third party storage service. There are several existing encryption methods such as Key Policy Attribute Based Encryption (KP-ABE) [7], Cipher text Policy Attribute Based Encryption (CP-ABE) [8] and Hierarchical Attribute Based Encryption (HABE) [9] is used to encrypt the user outsourcing details before uploading PHR to the third party in the cloud environment. These encryption processes ensure the security and data confidentiality using the public key encryption plans. Even though the public key encryption technique manages the security of the PHR records, the key management and scalability is a major issue during the authentication.

To address this issue Hybrid Patient Controlled Biometric Encryption Scheme (HPCBES) is used to manage the patient information in the cloud environment. The biometric encryption process linked with the Key Policy Attribute based Encryption techniques which consist of different image processing and encryption techniques. The biometric features are unique to each user that helps to recognize the user identities with fast, accurate. So, the proposed system uses the fingerprint [10] as the biometric feature because it has specific and unique ridges, valleys on the skin. The captured fingerprint processed by the image capture module, feature extraction and template matching mode. The extracted features are encrypted with the help of the encryption technique and those encrypted images are matched during the template matching phase. Then the Multiple Authority Attribute Based Encryption (MAAE) approach is used for granting the access control permission to the multiple users for sharing and accessing the PHR records in the cloud environment. The remaining of this paper is organized as follows. Section II discusses the related work; Section III presents the proposed system model; Section IV describes the performance evaluation and finally, Section V concludes our work in this paper.

## 2. RELATED WORKS

In cloud secure PHR data sharing is the important issues because it creates several securities and data confidentiality problem while accessing the cloud services. So, in this section describes the various discussions about the secure cloud PHR data sharing approaches. Ming Li et al., [11] propose an Attribute based Encryption system for managing the PHR data with scalable and secure manner. The proposed system uses the encrypted PHR data outsourcing approach for providing the fine-grained access control to the different users like public domain user and the personal users. Then the key management issue is overcome by using the dividing framework mechanism which monitors the multiple owners' access controls to establish the security with lower cost. The performance of the proposed system is evaluated with the help of the experimental results which achieves the scalable and secure PHR data sharing in the cloud environment. Danweiet al., [12] managing the multiple owner's security concepts during the PHR data sharing in the cloud environment. The multiple owners' security is monitored by dividing the users into different domains which reduces the complexity in the key management system. Then the patient privacy centric security is established by applying The Hierarchical and Multiauthority Attribute-Sets Based Encryption (HMASBE) approach. This encryption algorithm reduces the computational complexity and security while outsourcing the data in the third party storage device. Then the performance of the proposed system is evaluated with the help of the set up, key generation based experimental results.

*Rudrakshi* et al., [13] discusses the multi modal biometric system based encryption method to manage the user identities and important information in the cloud environment. The multi modal based biometric system ensures the authentication and creates the bio crypto system to manage the patient's personal information. The proposed multi modal biometric system reduces the hardware system cost and security cost in the cloud environment. *Pugazhenthi* et al., [14] multiple biometric features are used to manage the user entities in the cloud environment which leads to achieve the security while accessing the cloud services. This paper uses the fingerprints and related traits are used to establish the security to the user identities by using the RSA and Elliptic Encryption algorithm. The fingerprint biometric features are encrypted by applying the Elliptic encryption algorithm which is stored in the database and the templates are matched by RSA algorithm which improves the security in the cloud environment.

Ali A. Yasmin et al., [15] author develops the fingerprint recognition system for establishing the security to the user identities in the cloud environment. The captured user fingerprints are partially encrypted by applying the discrete wavelet transform and the encrypted images are stored in the database which is used during the template matching process. This encrypted and wavelet based verification scheme does not require heavy hardware and software requirements also does not need the largest amount. Thus, the author proposes the efficient fingerprint recognition system for verifying the user information and granting the access control permission while accessing the data in the cloud environment. Gandhi et al., [16] developing the secure, scalable and cost effective system for managing the user shared data. This paper uses the person unique biometric feature such as a fingerprint to authenticate the individual while sharing data or accessing data. The authentication system implements in the Automatic Teller Machine (ATM) and several public sectors and the performance of the system is evaluated by experimental results. Then the proposed system ensures the security while sharing the user information. So, the proposed system uses the fingerprint based biometric encryption system for managing the security while sharing the patient information (PHR) in a cloud environment. The following section discusses the detail proposed methodology.

## 3. PROPOSED METHODOLOGY

In this paper the user information security is managed by applying the Hybrid Patient Controlled Biometric Encryption Scheme (HPCBES) because the patient information (PHR) has several sensitive information. The PHR is created by the user which need to store in the cloud storage for accessing in the case of emergency. The shared information may be accessed by both public domain person like doctor, nurse, medical researcher and private domain person like user, family members and so on. During the information (PHR) accession process, the unauthorized user may try to access the private user information and modify those information’s which lead to create the problem for further processing. So, the security and fine-grained access permission is controlled by applying the biometric based encryption process. There are several biometric features are presented to controlled the security to the individuals, but the proposed system uses the fingerprint biometric feature to monitor the private user information. Each fingerprint based biometric system recognizes the authorized user with high accuracy with minimum cost and requirements also it is easily accessible in social. Thus, the fingerprint biometric image features are extracted by identification and minutiae detection process and those extracted features are encrypted with the help of the Self Healing Attribute based Encryption process. The encryption process creates the Bioscrypt which is stored as a template in the database.

Before is the above Bioscrypt generation process the user shared information’s (PHR) are encrypted by applying the Multiple Authority Attribute Based Encryption (MAAE) approach which used to granting the fine-grained access control and security while accessing the public domain user. The MAAE approach manages the multiple key management system by comparing the Bioscrypt template with the user fingerprint. The encryption and template matching process is performed after making the following arrangements.

### *Setup*

The first step is to arrange all the initial parameters which need to establish the security while sharing the data in the cloud environment. The initial parameters are public key *PK*, secret key *SK*, and private key generated by each authority attribute. Each attribute has information about the particular user.

$$\text{Setup } (1, N) \rightarrow \textit{via} \text{ (params, } \{(PK_k, SK_k)\}\ k \in \{1 \ldots N\})$$

### *Key Generation (MK, SK)*

The key generation algorithm uses the private key 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 attribute authorities.

$$\text{A Key Gen } (SK_k, GID, A_k) \rightarrow \textit{via } SK_k [GID, A_k]$$

Where,

**GID** – *user with identity*

**SK** – *Secret key*

**$A_k$** – *Attribute set*

After making this arrangement, the private key is generated by applying the biometric based encryption process. So, the biometric fingerprint features are extracted as follows to establish the security while sharing the PHR information.

### 3.1. Bioscrypt Generation using Self Healing Attribute based Encryption Method

After arranging the initial set up, the Bioscrypt images are generated by capturing the fingerprint of both the public domain and private domain user. The captured image features are extracted by using the two different modules like fingerprint identification and minutiae detection process which is explained as follows.

#### *Fingerprint Identification Process*

The Fingerprint identification process [18] is one of the authentication process. Each fingerprint has more number of points which can be varied from one person to another person. The fingerprints consist of dark lines and white lines, the dark line called as ridges and the white line called as the valleys. This dark and white line patterns have particular unique information which is used to authenticate the user. The changes of the ridge structure are commonly called as the minutiae and which can be grouped into three different types, Arches, Loops and Whorls. Generally the fingerprints are identified by applying the following steps, image acquisition; storing the image, image segmentation, image normalization and classification process. In this paper the image processing and feature extraction steps are used for ensuring the authentication of the cloud data sharing users and client.

#### *Fingerprint Image processing and Minutiae Feature Extraction*

The captured skeleton fingerprint images and the corresponding binary images have some unwanted holes; dot and island which lead extract the same fake minutiae from the skeleton image. So, before processing the image morphological operator is used to separate the same parallel valleys, fake bridges in the skeleton image. This process eliminates the noise, dots, lakes and fake islands from the skeleton fingerprint image. From the preprocessed skeleton image, the original minutiae features are extracted as follows.

#### *Minutiae Feature Extraction*

Minutiae features are an important feature which is used to compare the one skeleton image into the other image. The minutiae feature have included the Ridge ending, Ridge bifurcation, Short ridge, Island, Ridge enclosure, Spur, bridge, Delta and core. The automated minutiae identification and extraction process used to eliminate the fake minutiae point which is done by extracting those ridge points. The minutiae point extraction and corresponding orientation maps are ensured the robust authentication process during the template matching process also reduces the complexity while matching the patterns. The binary image minutiae feature extraction process consumes more time, complexity, low quality of the image also it loss some important features due to the reason the proposed system extracts the minutiae features directly from the grayscale image. In this paper, the fuzzy membership value is used to determine the minute feature range in the skeleton image. The dark (ridges) and white (valley) images are divided in the 5 × 5 matrix and the average value is calculated from the 25 values and the average boundary value also calculated which is considered as the dark and white fuzzy membership value. These two different average value considered as the linguistic variable which denotes to represent the brightness value. This dark membership value and Bright membership value determine the ending ridges from the grayscale skeleton image. This process reversed as the bifurcation detection process. The sample minutiae detected image is shown in the figure 1.

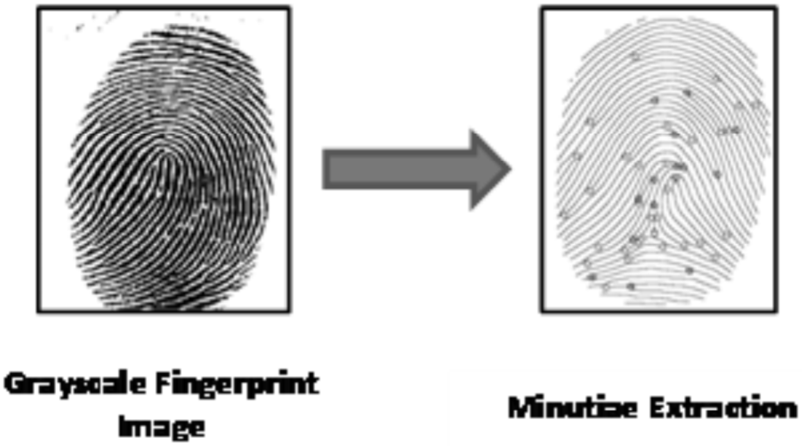

**Figure 1: Minutiae Extraction Process**

After extracting the minutiae features from the grayscale image, the Bioscrypt images are generated by encrypting those features with the help of the Self Healing Attribute based Encryption process. The encryption is done as follows,

Self healing [19] is one of the efficient multicast secure model which is used to update the key when the users changes continuously. The Self-Healing process encrypts the minutiae features into four different stages, namely broadcast; encryption and self-healing. The encrypted session keys $K_j$ are selected and broadcasted with the private key $d_{i.}$ Then the self-healing key $r$ has been selected within the session key range. $1 \leq r < j \leq m$. After choosing those keys, the encryption was performed as follows,

$$Cm_i = m_i \oplus H_2\,(e(d_i, Q_i)) \tag{1}$$

Where, $C_{mi}$ is the Bioscrypt feature value (encrypted feature value), $m_i$ is the feature belongs to the particular group of feature and $d_i$, $Q_i$ is the private key and self healing keys presents in the encryption process.

The self-healing is done after the encryption process with the help of the broadcast which is used to share the PHR data in the cloud environment. All minutiae feature present in the images are encrypted by using the broadcasted self-healing private key which improves the security while sharing the information in the cloud.

## 3.2. PHR Information Sharing in the cloud Environment

The next stage is PHR information sharing in the cloud environment, during the information sharing the Bioscrypt image is used to enhance the security. Information sharing is done in two different ways. The information may be shared via the patient side and doctor side which are explained as follows.

### *3.2.1. Patient Side Information Sharing*

The PHR information is created by the patient who is the responsible for creating, update the PHR information. The information needs to be stored or share in the cloud because the information may be accessed by the doctors in the emergency case. Before sharing the PHR information, the owner of the PHR data fingerprint need to be captured and it was encrypted by applying the Self-Healing Encryption process. This process encrypts the features and generate the Bioscrypt which updates their encrypts key while multiple user access the information. This Bioscrypt image used to authenticate the particular person while accessing the PHR data in the cloud. In addition, to improve the security the PHR data need to be encrypted before sharing the information. The encryption is done with the help of the Multiple Authority Attribute Based Encryption Process (MAABE) [19]. During the encryption process both patient and doctor uses the same public key and different private key for ensuring the security, data confidentiality and authentication. After the encryption the PHR data is stored in the cloud in a secure and scalable manner.

### *3.2.2. Doctor Side Information Sharing*

In the doctor side also, the doctor fingerprints are captured and generate the Bioscrypt image using the Self-Healing Encryption process which is used to authenticate while accessing the particular patient PHR data in the cloud. After accessing the patient PHR data, the doctor prescribed details also encrypted before sharing the information into the cloud. The encryption process is done with the help of the Multiple Authority Attribute Based Encryption Process (MAABE) which improves the security while multiple user accesses the information. The Bioscrypt and encrypted PHR data enhance the security during the information accessible. The PHR data encryption process is explained as follows.

### *3.2.3. Multiple Authority Attribute Based Encryption*

Multiple Authority Attribute Based Encryption (MAABE) process used to encrypt the each patient and doctor prescribed PHR details before sharing in the cloud environment. The encrypted data used to achieve the security while sharing the data in the cloud. The MAABE algorithm consists of multiple attribute authority and the multiple user, the user selects the attribute authority and uses the personal secret key to encrypt and decrypt the user PHR information. The algorithm consists of following initial steps, namely set up, create user, create authority, request attributes public key, request attributes secret key, encryption and decryption process.

#### *Setup*

The algorithm selects and generate the public key (PK) and private or master key (MK) of the system which used for encryption and decryption of PHR data.

#### *Create User*

Select the user (patient or doctor) who have both public key (PK) and a secret key (SK)

#### *Create Authority*

The authority is created based on the secret or private key which is used to encrypt the PHR data and decrypt the PHR data.

#### *Request Attributes Public Key and Private Key*

In this step each user public key and private key have been generated, the public key is known to everyone. After arranging these basic parameters, each data present in the PHR data has been encrypted by applying the user private key, secret key and public key and returns the cipher-text (CT) which is shared in the cloud via the internet. Then the decryption process is done by using the private key, cipher-text with a set of attributes. If the user attributes are satisfied with the particular private of key and secret key, then the particular patient PHR information may be acceptable.

### 3.3. Matching

The next step is a template matching process which is done by comparing the template stored in the database with captured fingerprint. This template matching process ensures that how the proposed system, enhance the quality while sharing the information in the cloud. The captured fingerprint minutiae features are extracted and separate the common candidate points, list the two common points and unconfirmed point. After extracting the those features the matching is performed by applying the decryption process which is done as follows,

$$Decrypt = C_{mi} \oplus H_2\left(\frac{e(d,U_k)}{e(HA,U_j)}\right) \tag{2}$$

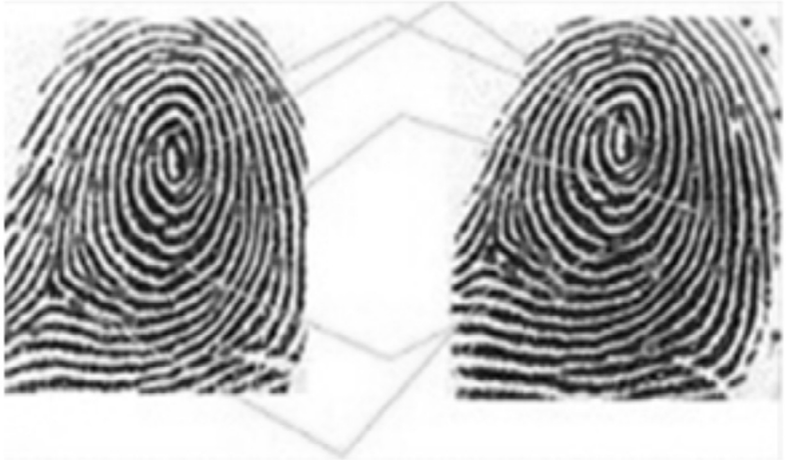

**Figure 2: Template Matching**

After applying the decryption process, the extracted features are matched with the input image and the template image for obtaining the authentication of the user which is represented as figure 2.

Thus, the proposed Hybrid Patient Controlled Encryption method ensures the security and authentication for patient and doctor shared PHR data.

## 4. PERFORMANCE EVALUATION

The proposed system ensures the security, authentication, authorization and data confidentiality using the fingerprint biometric based encryption methodology. The following parameters like Accuracy, Convenience, cost and size are used to how the proposed biometric feature helps to provide the security while accessing the cloud PHR data. In the proposed system CASIA fingerprint database is used to match the user while accessing the PHR data in the cloud. The fingerprint matching score obtained value is shown in the table 1.

**Table 1**
**Different Biometric Technology**

| *Technology* | *Accuracy* | *Convenience* | *Cost* | *Size* |
|---|---|---|---|---|
| Fingerprint | 10 | 10 | 2 | 3 |
| Voice | 6 | 7 | 8 | 5 |
| Face | 4 | 5 | 4 | 7 |
| Hand | 3 | 3 | 6 | 6 |
| Iris | 5 | 2 | 3 | 4 |

*1 (worst) – 10 (best)

From the above table the fingerprint biometric feature matches the various users with the highest accuracy. Then the biometric features are convenient to use while matching the user details with minimum cost and size when compared to the other biometric feature. Then the proposed system uses the fingerprint biometric feature for authenticate the particular user. In addition, to evaluate the performance of the system the security, efficient data sharing and authentication metrics are needed which is described as follows,

### *Security*

The security is achieved by encrypting the user details and fingerprint with the user defined private key and secret key which is difficult to hack by third parties because each fingerprint has unique characters which is encrypted by the self-healing key generation algorithm.

### *Efficient Data sharing*

The biometric features are used to authorize the user while sharing the PHR data in the network, in addition, the PHR data also encrypted by the particular authority attributes. So, it is difficult to hack the user shared information.

### *Authentication*

The user authentication is done by a template matching process, to improve the authentication process the stored templates are encrypted by self-healing which is only accessed by when the user having the related fingerprints, secrets and private key which is changed when the multiple user access the PHR data. So, the proposed system enhances the authentication while sharing the information.

Then the proposed system achieves the security and authentication with minimum key generation time and minimum execution time, which is shown in the figure 4 and 5.

From the above figure 4 clearly shows that the proposed HPCBES encryption algorithm consume minimum key generation time for different user when compared to different encryption algorithm. This fast key generation process executes the encryption process with minimum time and provides the security with the greatest manner.

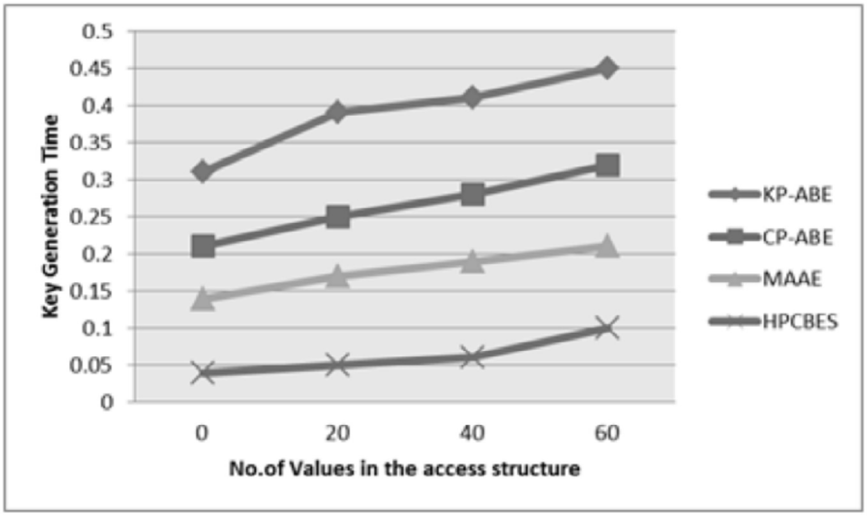

**Figure 3: Key generation time for different encryption techniques**

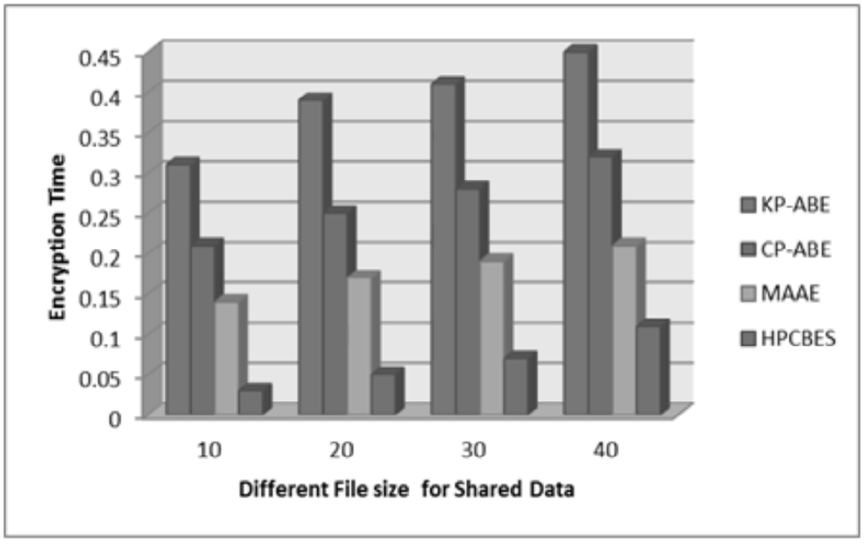

**Figure 4: Encryption time for different encryption techniques with Different shared file size**

Then the encryption time with different file sharing level of the proposed system performance is shown in the figure 5.

The above figure clearly shows that the proposed system encrypt the different PHR data size with minimum encryption time, which ensure the security of the PHR data with minimum time and achieves the efficiency while sharing the information.

## 5. CONCLUSION

This paper proposed the Hybrid Patient Controlled Based Encryption Scheme (HPCBES) to manage the security while sharing the PHR data in the cloud environment. The user fingerprint images are captured and the extracted minutiae features are encrypted by applying the Self-Healing encryption method and those images are generated by applying the Bioscrypt which stored as a template in the database for further matching process. In the proposed system CASIA fingerprint database is used for encryption and decryption process. Then, the PHR data is encrypted by using the Multiple Authority Attribute Based Encryption process to manage the key while multiple user accesses the shared PHR data. This double encryption process enhances the security while accessing the PHR data in the cloud. Then, the performance of the proposed system is evaluated with the help of the experimental results and discussion.

## *Reference*

[1] Sadiku, Musa, Momoh, “Cloud Computing: Opportunities and Challenges”, IEEEPotentials, Volume 33, Issue 1, 2014.

[2] PrajaktaSolapurkar, GirishPotdar, “A Survey on Secure Data Sharing and CollaborationApproaches in Cloud Computing”, International Journal of Science and Research, 2012.

[3] Harish Reddy, Venkat Reddy, JeevanaJyothi, “Security Issues in Cloud Computing Services”, International Journal of Advanced Research inComputer Science and Software Engineering”, Volume 3, Issue 6, June 2013.

[4] Eapen B.R., Chapman B. Mobile Access to Clinical Connect: A User Feedback Survey on Usability, Productivity, and Quality. JMIR mHealth and uHealth 2015; 3(2):e35.

[5] Charlotte Seckman, “Electronic Health Records andApplications for Managing Patient Care” Information Systems in Healthcare Delivery in Elsevier, 2013.

[6] Ming Li, Shucheng Yu, Yao Zheng, KuiRen,Wenjing Lou, “Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption”, IEEE Transactions On Parallel And Distributed Systems, 2012.

[7] Xiaolin Si, PengpianWang; Liwu Zhang, “KP-ABE Based Verifiable Cloud Access Control Scheme”, IEEE International Conference onTrust, Security and Privacy in Computing and Communications (TrustCom), 2013.

[8] LonghuiZu, ZhenhuaLiu; Juanjuan Li, “New Cipher text-Policy Attribute-Based Encryption with Efficient Revocation”, IEEE International Conference on Computer and Information Technology (CIT), 2014.

[9] Perumal, Rajasekaran, Duraiyarasan, “An efficient hierarchical attribute set based encryption scheme with revocation for outsourcing personal health records in cloud computing”, Advanced International Conference on Computing and Communication Systems (ICACCS), 2013.

[10] Sharma, Balasubramanian, “A biometric based authentication and encryption Framework for Sensor Health Data in Cloud”, International Conference on Information Technology and Multimedia (ICIMU), 2014.

[11] Ming Li, Shucheng Yu, Yao Zheng, KuiRen, Wenjing Lou, “Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption”, IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 1, January 2013.

[12] Danwei, Linling, Xiaowei, Liwen, “Securing Patient-Centric Personal Health Records Sharing System in Cloud Computing”, IEEE Communication Journal, Volume 11, Issue 13, 2014.

[13] Rudrakshi, Hatture, “A model for secure information storage and retrieval on cloud using multimodal biometric cryptosystem”, International Conference on Computer and Communication Technology (ICCCT) in IEEE, 2014

[14] Pugazhenthi, SreeVidya, “Multiple Biometric Security in Cloud Computing”, International Journal of Advanced Research in Computer Science and Software Engineering”, Volume 3, Issue 4, April 2013.

[15] Ali A. Yassin, “Efficiency and Flexibility of Fingerprint Scheme Using Partial Encryption and Discrete Wavelet Transform to Verify User in Cloud Computing”, International Scholarly Research Notices, Volume 2014, 2014.

[16] Sugandhi,Mathankumar, "Real time authentication system using advanced finger vein recognition technique", International Conference on Communications and Signal Processing (ICCSP), 2014.

[17] Le Hoang Thai and Ha Nhat Tam, "Fingerprint recognition using standardized fingerprint model", International Journal of Computer Science Issues, Vol. 7, Issue 3, No 7, May 2010.

[18] Yixin Jiang, Chuang Lin, Minghui Shi, Xuemin, "Self-healing group key distribution with time-limited node revocation for wireless sensor networks", Ad Hoc Networks in Science Direct, 2007.

[19] Fei Li, Rahulamathavan, Rajarajan, "Low Complexity Multi-authority Attribute Based Encryption Scheme for Mobile Cloud Computing", IEEE International Symposium on Service Oriented System Engineering (SOSE), 2013.