**International Journal of Computer Engineering & Technology (IJCET)**
Volume 10, Issue 1, January-February 2019, pp. 72-80, Article ID: IJCET_10_01_009
Available online at
http://iaeme.com/Home/issue/IJCET?Volume=10&Issue=1
Journal Impact Factor (2016): 9.3590(Calculated by GISI) www.jifactor.com
ISSN Print: 0976-6367 and ISSN Online: 0976–6375


# EXPERIMENTAL STUDY ON CLOUD SECURITY FOR PERSONAL HEALTH RECORDS OVER PATIENT CENTRIC DATA

**Birru Devender**
Research Scholar, Rayalaseema University, Andhra Pradesh, India

**Dr. Syed Abdul Sattar**
Director Research and Development,
Nawab Shah Alam Khan College of Engineering and Technology, Telangana, India

**ABSTRACT**

*Cloud computing offers many services among one is Storage as a service. Using this service user can outsource his data and whenever required he can download or he can share with others. Using cloud computing PHR owner can share his documents, but due to security challenges in cloud computing the health records of owner must be encrypted before outsourcing. In order to provide security for owner health records ABE (attribute-based encryption) is best suitable for other encryption techniques. Using ABE the PHR owner can define access control over his encrypted cloud data. But using ABE dynamic polices over encrypted cloud data is big challenge. In this paper for achieving grant and revoke privileges over encrypted data Timestamp server is introduced.*

**Keywords:** ABE, CP-ABE, PHR, IBE, DriveHQ.

**Cite this Article:** Birru Devender, Dr. Syed Abdul Sattar, Experimental Study on Cloud Security for Personal Health Records over Patient Centric Data, *International Journal of Computer Engineering and Technology,* 10(1), 2019, pp. 72-80.
http://iaeme.com/Home/issue/IJCET?Volume=10&Issue=1

## 1. INTRODUCTION

Now a day's Cloud Computing is emerging solutions for storing and sharing of information in the cloud environment, where computing resources including process and storage is provided by a third party service provider i.e. they are semi-trusted in domain thus raise serious concern of individual privacy for the Adoption of cloud computing technologies. Where in the presented system in order to privacy protection concerned surveys of research categorized as privacy by policy, privacy by statistics, and privacy by cryptography applied on various public and personal domain. However, the privacy concerns and data sharing requirements on different parts of the medical data may be distinct ways it losses data integrity and authenticity when data are encrypted using an (Attribute Based Encryption)ABE scheme

under KP-ABE and CP-ABE , key management is difficult if there is access levels are more from various backgrounds where in Health Domain . Now a day's Cloud Computing is emerging solutions for storing and sharing of information in the cloud environment, where computing resources including process and storage is provided by a third-party service provider. Generally CSP offers various services to the clients like IaaS (Infrastructure as a Service), PaaS (Platform as a service), SaaS (software as a service) DaaS (Database as a service) using these services without local maintenance the client can consume these service pay-as-you like Storage service offering by Amazon EC2, IBM, Microsoft and Rockspace etc . Cloud can deployed in four ways private cloud, public cloud, hybrid cloud and community cloud. The public cloud can utilized by any client due to this security challenges the document must encrypted before uploading and due public available of document the data integrity required using data integrity the client can know the status of his data weather data is modified or not. But due to privacy of cloud data many cryptography techniques are implemented, using cryptography techniques managing secrete keys are difficult Where in the presented system in order to privacy protection concerned surveys of research categorized as privacy by policy, privacy by statistics, and privacy by cryptography applied on various public and personal domain. However, the privacy concerns and data sharing requirements on different parts of the medical data may be distinct ways it losses data integrity and authenticity when data are encrypted using an (Attribute Based Encryption) ABE scheme under KP-ABE and CP-ABE, defining fine grained access structure over cloud data is difficult and key management is difficult if there is access levels are more from various backgrounds where in Health Domain.

## 2. PROBLEM STATEMENT

Generally PHR system has multiple PHR owners and PHR users. The owners refer to patients who have full control over their own PHR data, i.e., they can create, manage and delete it. There is a central server belonging to the PHR service provider that stores all the owners‟ PHRs. The users may come from various aspects; like, a friend, a caregiver or a researcher. Users access the PHR documents through the server in order to read or write to someone's PHR, and a user can simultaneously have access to multiple owners‟ data. Correctness of the PHI in the cloud is put at risk due to the following reasons. Although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they still face a broad range of both internal and external threats to data integrity. Outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large-scale data storage, it does not offer any guarantee on data integrity and availability. This problem, if not properly addressed, may spoil the successful deployment of the cloud architecture. Our Proposed work is to improve the privacy preserving PHR framework utilizing Attribute Based Encryption (ABE) with fine-grained approach with precise (accurate) time stamp Server for reliable patient data.

## 3. RECOMMENDED SYSTEM

This probe concentrates user separateness instant outsourcing their data in muddle cache structures, a user may hold refers disseminated by legion authorities and the landowner may split data with users administrated to strange authorities. For occurrence, in an E-health process, the medicinal data may be experienced only with a user who has the trace of "Doctor" promulgated by an institution and the apply "Medical Researcher" televised by a pharmaceutical testing ground. Some CP-ABE schemes have been recommended for such multiauthority organizations. However, by virtue of the disorganization of calculation, they cannot be instantaneously perturb build up the data connection administer scheme. Basically,

skillful are two operations in approach govern that involve active reckoning, i.e. homespun manner and thick method.

The key idea sniff out slice management into legion freedom domains consider bypass from high key care intricacy respectively proprietor and user (specifically, community domains and personal domains (PD)) just as the original users' data way involvements.

### 3.1. Personal Domain (PD)

Personal Domain is used for Outsourcing the data by the data owners, data owners initially encrypts the data with content keys by using symmetric encryption techniques. Then, the owner defines the access policies with timestamp over attributes from multiple users and encrypts content keys under the policies. They do not trust on the server to do data access control. Instead, they assume that the server may give the data to all the users in the system. But the access control happens inside the cryptography. That is only when the user's attributes satisfy the fine-grained access policy with time stamp defined in the ciphertext and satisfied by the fine-grained policy; then user is able to decrypt the ciphertext for the sake of Read or Write or Read-Write Operations.

### 3.2. Public Domains (PUD)

The PUDs consist of users who make access based on their professional roles, such as doctors, nurses, and medical researchers. In practice, a PUD (Public Domains) can be mapped to an independent sector in the society, such as the health care, government, or insurance sector. For each PSD, its users are personally associated with a data owner (such as family members or close friends), and they make accesses to PHR (Patient Health Record) s based on access rights assigned by the owner

**Timestamp Server:** Time stamping service is primitive service in our methodology which protects data confidentially by providing data availability in Cloud Server with a specified time frame afterword's data will be unavailable once time excides which protects high security by data availability.

## 4. SCOPE OF RESEARCH WORK

To secure the PHR in a cloud computing, we propose a secure patient-centric PHR access-based concept. Within health domain can access the health records, unauthorized users can't access the owner's personal health records. After giving Access control to health records the PHR owner can affectively revoke the user at any time, and if any attribute policies changes to the user the attributes policies update by TTAA.

In this analysis a completely unique Dynamic Time based mostly encoding and searchable access management theme are attending to be gift and during this method 3 completely different entities are concerned like PHR owner, PHR users and Attribute authorities.

PHR owner: Who wish to share his personal health info through cloud?

Attribute authorities: Who can take attributes from users and generate as key and personal key.

PHR users: Who wish to transfer Personal health info from cloud?

*The analysis work enforced as follows:*

The PHR owner can source his Personal health record to the cloud so as to share with others however because of privacy reasons the PHR owner ought to write in code the PHR before outsourcing.

The PHR owner can take the attributes from multiple authorities and he can write in code the PHR by victimization public key, whereas generating public key he can add time stamp to

the every attribute. therefore once encrypting he can transfer to the cloud same approach so as to modify searchable encoding to the PHR users the PHR owner can outline keywords to the every PHR and so as to privacy he conjointly encrypts the keywords and he can transfer to the cloud. Therefore, so as to look any PHR in cloud the PHR user should get searchable permissions from cloud. Attribute authorities are accountable for managing attributes, they're going to take attributes from completely different users and same approach they're going to generate secrete key for PHR users.

PHR users: so as to transfer any PHR from cloud the PHR user should submit their attributes to the any attribute authority and for downloading PHR the user should get search request from corresponding PHR owner, therefore once obtaining search response the PHR user will able to search PHR from cloud, therefore once downloading the PHR, for decrypting the user can use his secrete key.

## 5. RESULT AND ANALYSIS

The Entire experiment were carried out in three operations first File encryption and decryption, second File upload and third policy update or revoke. DriveHQ Drive Headquarters Inc, it is a one of the cloud service provider, and it provides storage as a service, using this PHR owner can store and share his data. Drive HQ Home page using this PHR owner need login, in order to login the PHR owner first must register with service provider

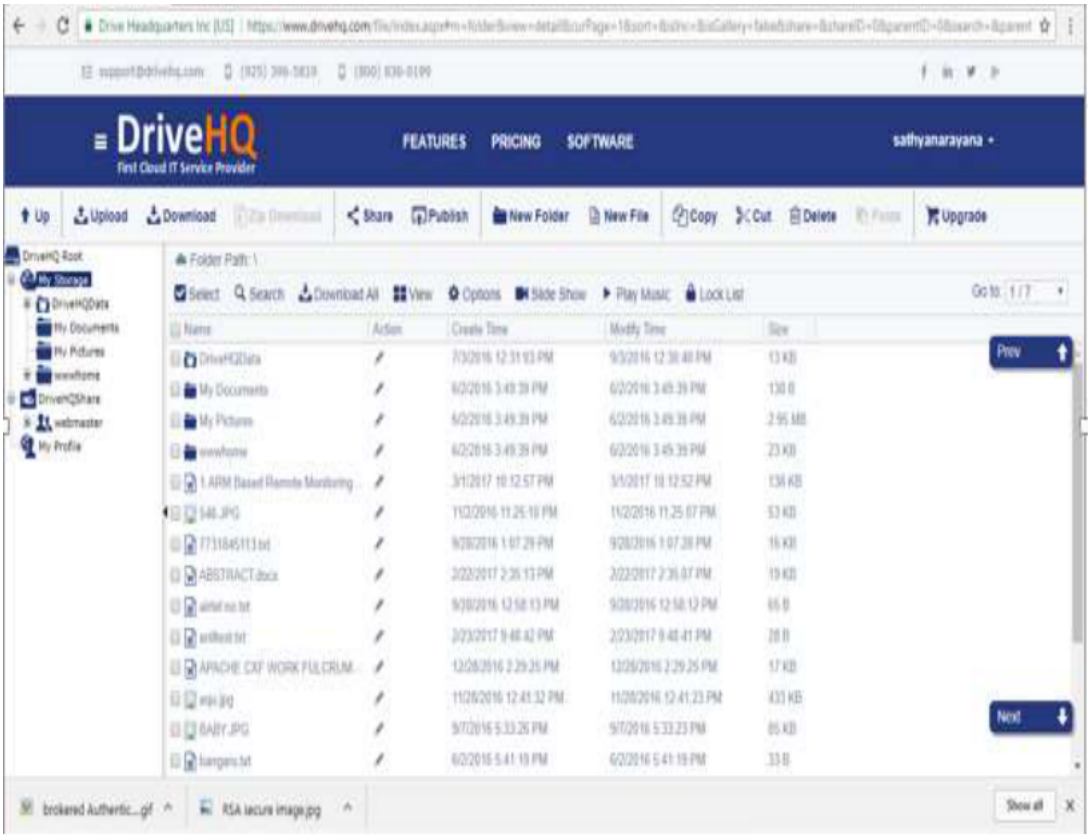



**Figure 1** DriveHQ home page

This is the home page of DriveHQ, here PHR owner can view his uploaded documents.

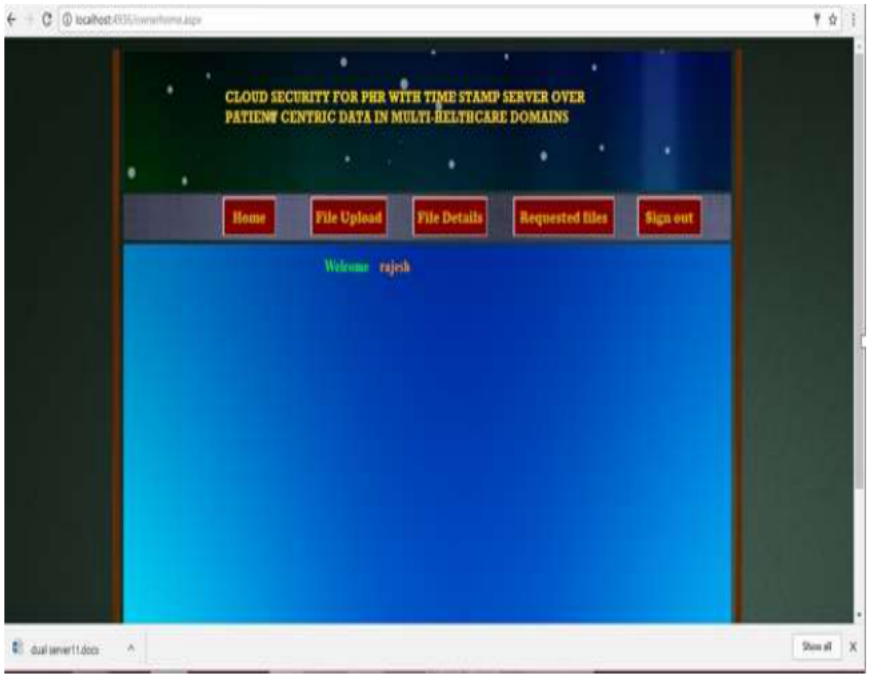



**Figure 2** Patient Home page

After login patient can perform following operations like he can upload file, he can view files which are uploaded earlier and he can grant or revoke permissions of requested file.


**Figure 3** File upload

Here patient can upload his document to DriveHQ, for this he required file id, file and timestamp.

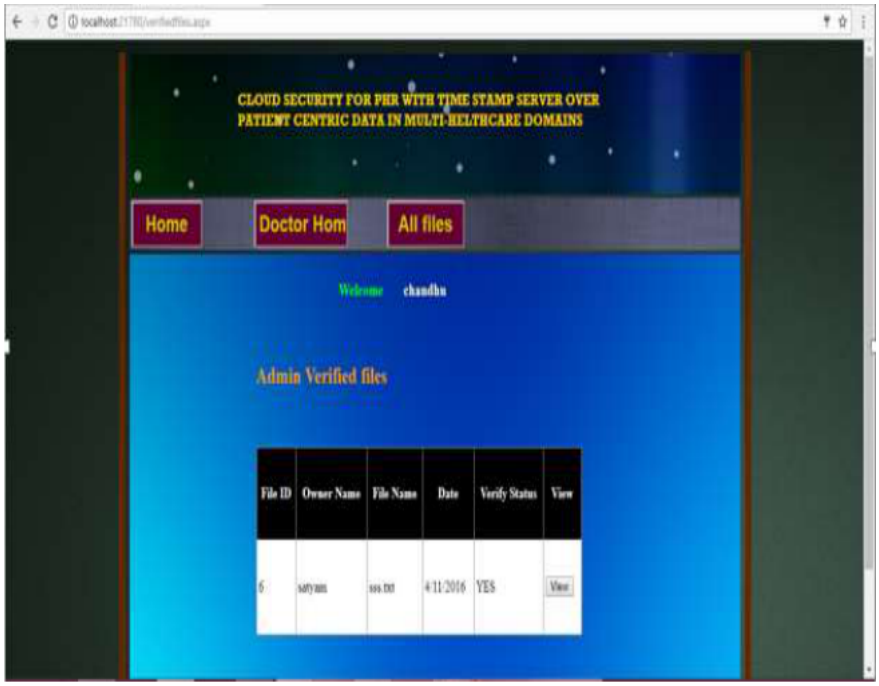



**Figure 4** Doctor Home page

Using this page the doctor can view patient records or documents. And if any record he ant to download then he must get permissions from record owner.

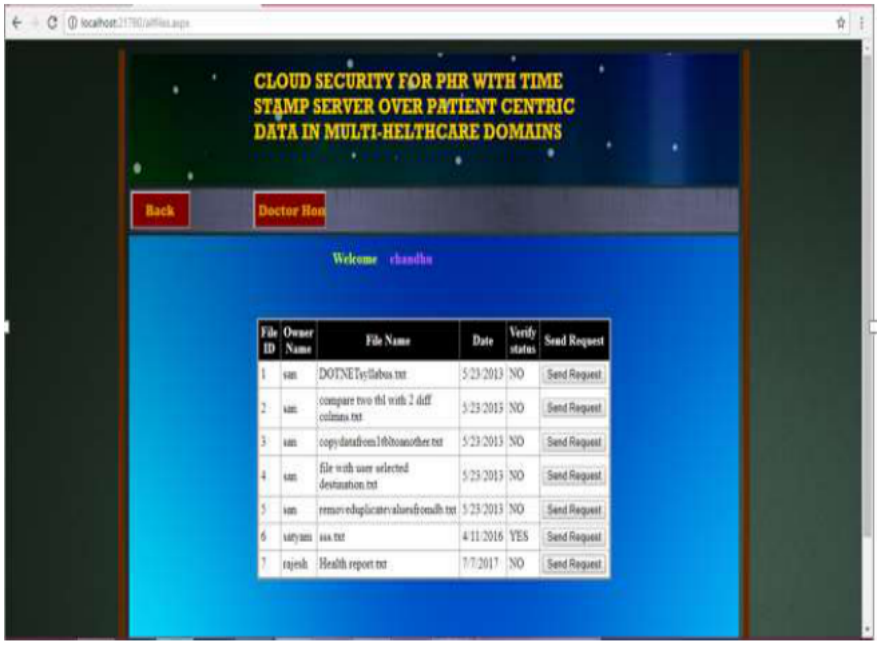



**Figure 5** Doctor Requesting for Record

Here the doctor can send request for particular record in order to download the record he must get permissions from record owner.

In cloud users uploading file to the cloud in order to that they must generate policy like who can decrypt or not, in below graph policy time calculated for different attributes.

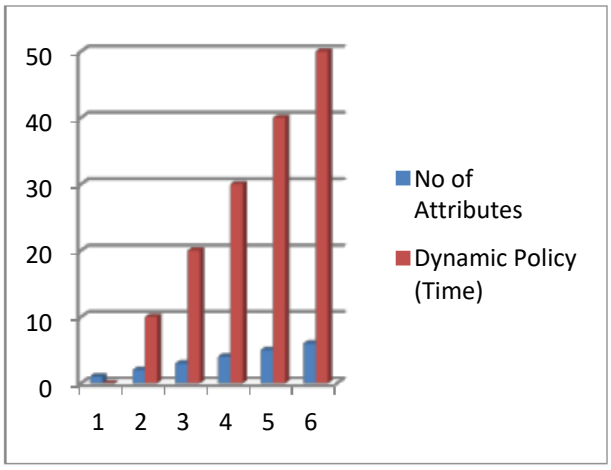



**Figure 6** Policy generation time

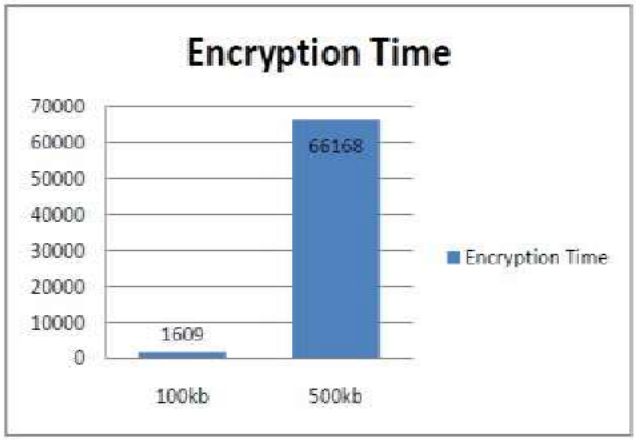
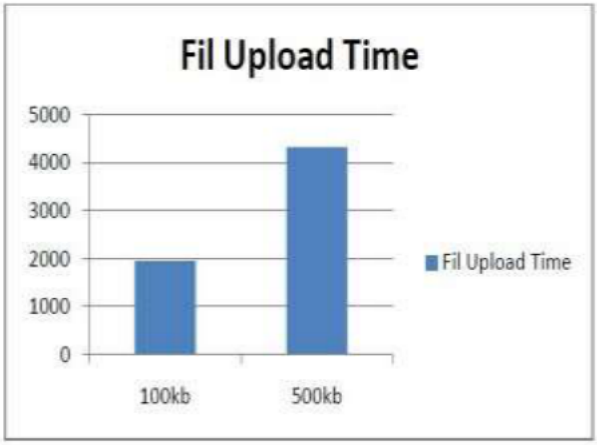



**Figure 7** File encryption time for different File sizes



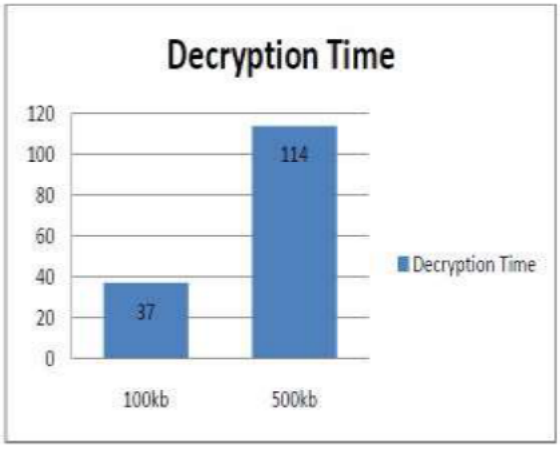




**Figure 8** File uploads time for different file sizes **Figure 9** File decryption time for different File sizes

Policy generation done by CP-ABE algorithm in below graph describes comparative time for policy update or revoke for different users calculated.

A user uploading files to dropbox and it allowing users for achieving various functions. To measure the efficiency of different file sizes, data with variable sizes ranging from 100kb to 500kb is selected.

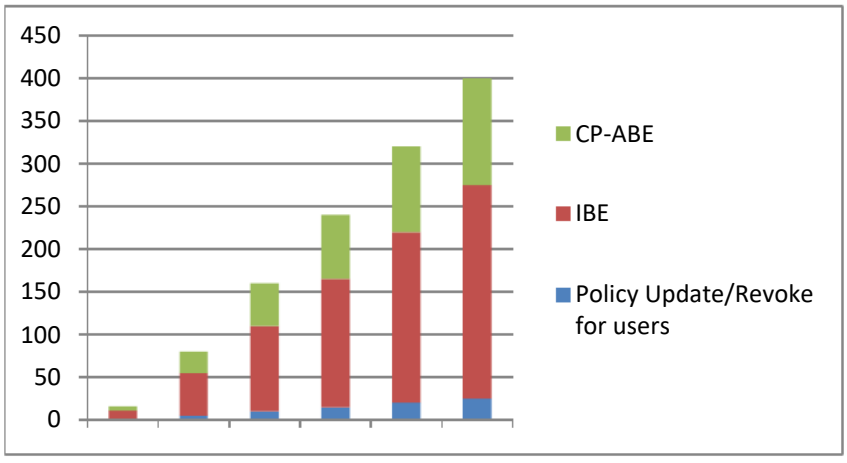



**Figure 10** Policy update/revoke comparative analysis between IBE and CP-ABE

There are many operations are done in this experiment. The users can login and register to the homepage for uploading and downloading the files. The start time for uploading and the finish uploading time is calculated resulting in the total upload time. And same way Encryption and decryption of different file sizes with time calculated.

## 6. CONCLUSIONS

In this work proposed time stamp server over patient centric data in multi-health care domains where group of doctors and patients share their personal heath records. This work will improve PHR framework efficiency and Privacy among multiple authority access and it achieves Revocation of forward and backward security with help of timestamp server. The PHR owner can efficiently define access police over his data. Timestamp will generate dynamic keys based on user request. To overcome Limitations of research work, Future scope of work is new novel concept called Dynamic Time-based Asymmetric encryption (DTBAE). The TTA the trusted third party auditor will generate secrete keys to the users if any user policy changes without updating entire document or without changing every user keys the TTA will grant new keys to the users. a novel algorithm is proposing is called DTBAE dynamic time-based asymmetric encryption which generates new secrete keys to every user whenever policies changes or if any user giving request for particular it generate the secrete keys and same way based on access structure.

## REFERENCES

[1] Anna Sachinopoulou, Ontology-Based Approach for Managing Personal Health and Wellness Information", Engineering in Medicine and Biology Society, EMBS 2007. 29th Annual International Conference of the IEEE, pp.569-571, 2007.

[2] Ajmal Sawand, Toward energy-efficient and trustworthy eHealth monitoring system", Volume 12, Issue 1, pp.46-65.2015.

[3] Cheng-Yi Yang & Chien-Tsai Liu (2013), "Developing IHE-Based PHR Cloud Systems", Social Computing (SocialCom), International Conference on, pp.1022-1025, 2013

[4] Chia-Hui Liu, "Secure PHR Access Control Scheme for Healthcare Application Clouds", Parallel Processing (ICPP), 42nd International Conference on, pp.1067-1076, 2013

[5] Danwei Chen, "Securing patient-centric personal health records sharing system in cloud computing", Volume: 11, Issue: 13, pp,121-127, 2014.

[6] Florian Daniel, Beyond Health Tracking: A Personal Health and Lifestyle Platform", Volume: 15, Issue: 4, pp.14-22, 2014.

[7] Jun Zhou, "PSMPA: Patient Self-Controllable and Multi-Level Privacy-Preserving Cooperative Authentication in Distributedm-Healthcare Cloud Computing System", Volume: 26, Issue: 6, PP: 1693-1703. 2015,

[8] Kaitai Liang & Willy Susilo, "Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage", Volume: 10, Issue: 9, pp.1981-1992. 2015,

[9] Lan Zhou, "A Secure Role-Based Cloud Storage System for Encrypted Patient-Centric Health Records", Volume: 59, Issue: 11, pp.1593-1611. 2016.

[10] Prasadu Peddi, Design of Simulators for Job Group Resource Allocation Scheduling in Grid and Cloud Computing Environments, Volume 6, Issue 8 pp.17805-17811. 2017

[11] Prasadu Peddi, Data sharing Privacy in Mobile cloud using AES, Volume 7, Issue 4. 2018.

[12] Randike Gajanayake, "Sharing with Care: An Information Accountability Perspective", Volume: 15, Issue: 4, pp.31-38. 2011.

[13] Shu-Di Bao; "A Method of Signal Scrambling to Secure Data Storage for Healthcare Applications", Volume: 21, Issue: 6, pp.1487-1494. 2017

[14] Yin Zhang; "Health-CPS: Healthcare Cyber-Physical System Assisted by Cloud and Big Data", Volume: 11, Issue: 1, pp: 1-5, 2017.