ISSN: 0369-8963

A Novel Cryptography Technique for Securing Personal Healthcare Record

J. VIJILA [1*], A. ALBERT RAJ [2]
[1]Corresponding author, University College of Engineering, Nagercoil, India.*
[2]Sree Krishna College of Engineering and Technology, Coimbatore, India.

Abstract

Personal Healthcare Record (PHR) is an emerging patient-centric paradigm for exchanging health information in the cloud. Individuals' medical records are kept and backed up using this technology. As a result, this data is often transferred to a third-party service provider, such as a cloud service provider (CSP). As a result, this data may be accessible to third-party servers and to unauthorised persons. Personal healthcare information may be securely shared in the cloud utilising Elliptic Curve Cryptography (ECC) method, which ensures Patients have ownership over their own personal health information. Based on the user's rights, a method called multiple data file partitioning is utilised to divide the data file. The ECC encryption method is used to secure the partitioned data file. Public and private keys issued by the key issuer are required for access to the PHR by data owners and users. A private key is also required for the decryption procedure. Hence, the PHR are protected from unauthorized users and barred attackers and thus the proposed model improves data privacy, access control, efficiency and scalability when compared to existing model.

Key words: *PHR, Cloud computing, CSP, ECC, Multiple file partitioning, Unauthorized attacks.*

Introduction

With cloud computing, computer system resources may be made available on-demand, just for the purpose of storing and processing data, without requiring the user to take any action. Vast number of individuals can access the data centre over the internetare often referred to as "cloud computing." Administrators who are not acquainted with cloud pricing structures may run into unanticipated costs while using a provider's "pay-as-you-go" archetype. As one of the most essential aspects of the cloud, cloud storage is utilized for a wide range of sensitive data, including Personal Health Records (PHRs), Organizational Records (ORs), and Government-Related Data (GRD). Patients may use multi-owner settings in an online PHR to centrally control their own medical record and summary. Every domain of PHR may be accessed with fine-grained control. ABE is used to encrypt domain-based Personal Health Records (PHRs) that are within the control of their owners. [1].

PHR are often outsourced to Cloud Service Providers (CSP), it may cause several attacks due to third-party service provider (unauthorized parties). Furthermore, the most critical consideration while storing and transferring PHR to the cloud is security. Applying encryption technologies to only provide the data decryption key to trustworthy authorized users would help keep sensitive data secret against untrusted servers. Security, scale and fine-grained control over the untrusted cloud are provided by the unique combination of ABE, proxy re-encryption, and lazy reencryption. The safety of cloud computing has become a hot subject in both business and academia.Virtualization security is the most important factor that is accomplished by digital signature [2].

 https://doi.org/10.37896/pd91.3/91341

ISSN: 0369-8963

PHR must be shielded from the general public by the security system in place. In order to ensure security, the cloud offers dynamic changing of access rules or file properties, facilitates quick on-domain user revocation, and provides break-glass access in an emergency event. Applications transactions are being earned by third-party providers because of their rapid growth and the requirement for massive servers and data centres to handle them in a timely manner.So, the valued cryptography method is needed to secure the computing applications [4].

Maintaining the confidentiality of sensitive user data in the face of potentially malicious servers. Access privilege secrecy and top-secret key liability for users are both preserved. Double-check the encryption of sent data by being acquainted with two separate encryption schemes. Key-Policy Attribute-Based Encryption ensures a second layer of protection for your sensitive data (KP-ABE). Each cipher-text in KP-ABE is given a descriptive file attribute as well as a private key as part of an access policy. [5] and [6] is attached to it.To Moderate some security risks, proper cryptography measure will be rise to taken. Proper delegation must apply to exchange the PHR details in cloud. So, there is a need to categorized the PHR. The prioritized level-based encryption and Multi Authority Attribute-Based Encryption (MA-ABE) take placed to secure the PHR in cloud [7].

Multiauthority Ciphertext Policy Attribute-Based Encryption (CP-ABE) scheme with user accountability is used to create a PHR sharing mechanism based on attributes. It uses to manage the user accountability in the PHR cloud. User accountability may rise computational overhead so, the system must use the set of policy and authentication [8]. For secure the PHR file, dual security is introduced between encryption and stored data. To encrypt the PHR data and provide extra confidentiality, progressive based encryption is utilised. And cloud security is assure using dual security. Dual signature security is used for transmission and storing PHR data in cloud with integrity [9]. When it comes to protecting PHR privacy, it is also important to keep in mind that recipients may have personal or medical information in their PHRs that should be kept private. Use of advanced anonymous attribute-based encryption (AABE) ensures the security of the PHR owner, but also protects privacy for those who receive it, and Two-factor authentication (2FA) is a cloud computing service area control system that authenticates both users and owners. [10], [11].

In cloud computing, the healthcare sector models cost-off storing, maintaining, and updating with enhanced efficiency and service quality. PHR are often distributed to internet for transmission between entities. In, medical trade, patients' treatments are provided by different segment. This enables the serious patient medical information is must be preserved and shared securely. The PHR are categorized by the sensitivity of the medical data and the separately secured by well good cryptography and key management techniques [12], [13]. It is becoming more common for a single application to need numerous encryption keys, which adds to the complexity of key management. Patients full control over their own PHR meets uses the key management. Encryption techniques for security and reliability of the PHR files. However, in real-life applications, privilege-based setting is most suitable solution for the PHR file [14], [15].

Related works

To ensure and secure the confidentiality of the PHR encryption techniques are used, like ABE [1], [3], [5], [8], [9] it's a most commonly used encryption technique and also we research the various cryptographical [12], [13] methodology that are all proposed by different authors related to our proposed model.

Li et al., [1]to develop a PHR data access control system that is patient-centered and fine-grained in its use of multiple owners' data They use the ABE technology to encrypt each patient's personal health record and the MA-ABE to deal with the complex policies. To simplify

 https://doi.org/10.37896/pd91.3/91341

ISSN: 0369-8963

key distribution, they divided the system into multiple security domains, each of which retains a specified portion of the user population. As a result, each patient has complete privacy control, and the administrative load is greatly decreased. It also allows for fast and on-demand revocation of user access controls, making their proposed system adaptable while also protecting break-glass access in the event of an emergency. Gampala et al., [2] propose a data security for ensure sharing sensitive data in cloud computing. This paper is determining the data security for data exchange in cloud computing by applying encryption and also use digital signature to provide authentication and confidentiality of data between clouds. Zheng et al., [3] PHRs may be shared and made secure on semi-trusted servers using the patient-centric approach. PHR files of individual patients are being encrypted using the ABE method to preserve privacy. Using this method, PHR owners may create custom, finely-grained access controls for their PHR files during encryption. Improved security is provided by the MA-ABE approach, which is also used to avoid the issue of key storage.

We suggest an authoritative factor of key length for cloud computing data sharing, as proposed by Alowolodu et al [4]. In addition, this system offers a common tool to model a secure platform for cloud applications. Using fine-grain data access control, Jothi et al. [5] present a cloud computing solution for securing and scaling data in the cloud. It protects users' private information from untrusted servers. Access privilege secrecy and top-secret key liability for users are both preserved. ABE and the proxy re-encryption mechanism are no more. One of the most effective and safest archetypes proposed is one that is demonstrably efficient and secure.

A cloud-based EHR, as proposed by Rakesh [6], will provide better security for Indian healthcare providers. In this system, the transmitted and stored data are protected by separate encryption algorithms.Progressive based encryption is used to encrypt the data. Elgamal algorithm is secondhand for text encryption and key generation. In this system has dual data security for transmission and storing data.

Sangeetha et al., [7] uses prioritized level-based encryption by improving the security of the PHR system in the cloud. The Prioritized Level-Based Encryption (PLBE) approach encrypts both text and picture data, such as x-rays and scans, in individual patients' Personal Health Records (PHRs). To protect both text and image data, a variety of encryption methods are needed. For multiple data owner scenarios, this method splits PHR users into several security domains for scenarios with numerous data owners, making key management more efficient for both owners and end-users.

To design an attribute-based PHR sharing scheme with user accountability, [8] proposes MA-ABE and CP-ABE schemes with user accountability. The user's privacy is protected because the access policies are hidden in the system. By revealing a PHR user's global identity and how he swindled other illegal users out of the decryption key, the authorities' and PHR users' trust in each other is diminished. The system is more secure and efficient when it comes to cloud-based PHR sharing.

Using cloud security in EHRs for Indian healthcare, Deshmukh [9] makes a compelling case. Double data security is provided because it familiarises the user with the isolation of encryption schemes. Each patient's Personal Health Record (PHR) file is encrypted using ABE. Secret keys for users were generated with KP-ABE. Large numbers of owners and users are made easier to manage by reducing the complexity of the key management. It has been proposed that PHR can be shared in the cloud while maintaining privacy and security, according to Zhang and colleagues [10]. Using Anonymous Attribute Based Encryption, they were able to keep PHR data private and secure while also enabling granular control over who could see what portions of those files in the public cloud (AABE). The public key is short, and the private key is always the same size. As a result of this, the standard model achieves compact security in the first order groups.

 https://doi.org/10.37896/pd91.3/91341

ISSN: 0369-8963

Two Factor Authentication (2FA) access control is proposed by Liu et al. [11] for the cloud computing service area. Both a user's secret key and inconsequential security devices were employed in an attribute-based access control system. Many e-banking services employ two-factor authentication (2FA) on a regular basis. It allows for a variety of different access methods depending on the situation.Hash function generate numbers that well-defined over finite field. 2FA access control system that anticipated security requirements.

Arunkumar et al., [12], Zanghloul et al., [13] propose a new knowledge to secure the images and data of patient's record. Extra care must be made to protect PHR photos and files since they make up the majority of the data in the system. You can do so with this system by transforming the images to pixels and then encrypting those pixels. Individual encrypted files are divide into n files and cloud storagewhen the encryption process is complete. Symmetric key cryptography is used to protect cloud server data.

The Electronic Healthcare Record (EHR) concept proposed by Sharaf et al. [14] is safe and efficient (EHR). CP-ABE is used to safeguard the EHR. As a patient, you have greater freedom to set access policies based on the attributes of data users and ensure that only authorized individuals have access. Using symmetric key cryptography, Shaikh [15] propose the safe exchange of Personal Health Records (PHR) via cloud computing.This system provides the extra modular policy for security and consider access control towards the PHR in cloud.

Even though the various authors propose so many algorithms and technologies there is a lack in security and nonexistence in key management. Hence, to improve further ECC algorithm is used in order to improve the security and in addition to key administration.

Proposed Work

Framework for secure and scalable ECC based model

To address the issue of safe data transfer, this solution employs the Elliptic Curve Cryptography (ECC) algorithm. ECC is an asymmetric encryption method that uses the algebraic structure of elliptic curves over finite fields to generate cryptographic keys that are faster, smaller, and more efficient. ECC uses the features of elliptic curve points and equation rather than the usual method of obtaining keys by multiplying very big prime numbers. Due to the fact that ECC helps to provide equal security with reduced computer and battery resource utilization, as well as robust key exchange characteristics.In other words, our architecture offers a secure PHR system that is easy to use while yet allowing for safe data transfer. Fig 1 depicts the ECC-based model's suggested framework.

In proposed framework, there are multiple data owners, multiple users and multiple authenticators (important components). In addition, ECC algorithm is used to secure the individual patients PHR. The data owner has the access control of read, write and upload PHR (representative of hospital or industries). System setup and key distribution are managed by trusted key issuer. The PHR file are accessed by data user with the secure decrypted key. The curve values are used to generate the keys. Public and private keys are used separately for upload a PHR and view or download the PHR. Any unauthorized attacks are possible the key issuer have the capability to remove or block the user. Here, the individual components working process explained based on our proposed model.

 https://doi.org/10.37896/pd91.3/91341

ISSN: 0369-8963

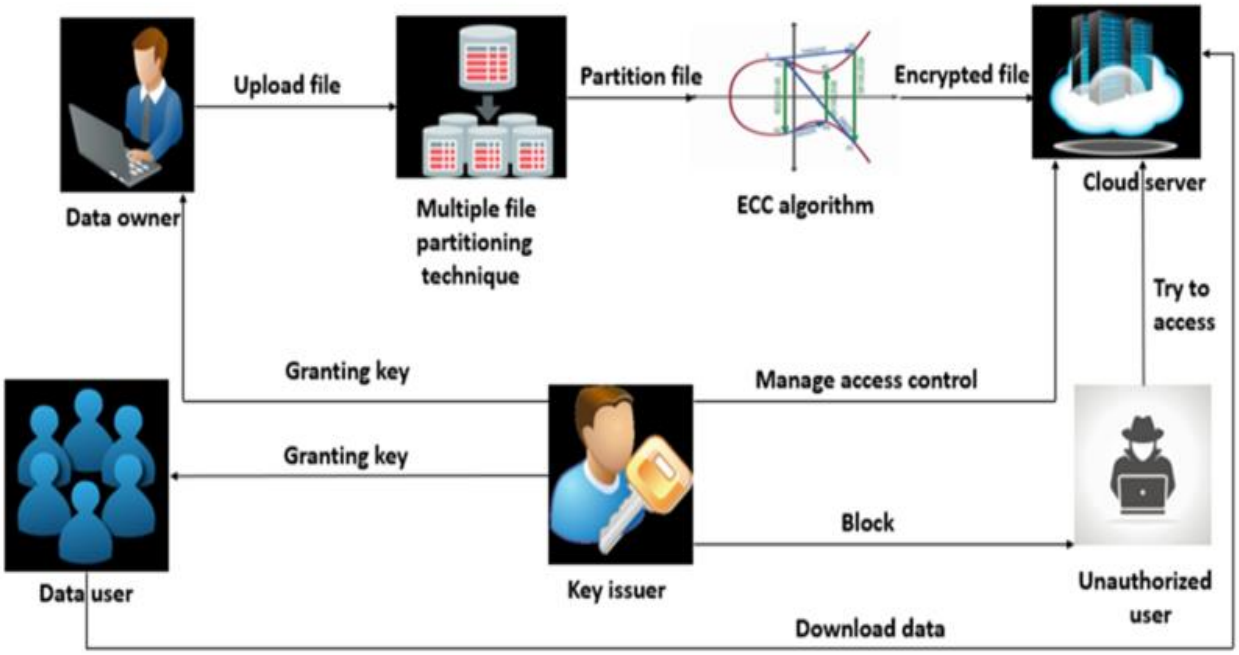


Fig. 1 The Proposed framework for secure and scalable ECC based model

Data owner

Data owner is an individual who is accountable for a data assert. If data owner is a new user, he/she must register in the PHR system, or data owner is already a registered user then login the PHR system with the use of username and password. Data owner is a main entity, they (data owner's) only have the capability to upload, update your PHR file based on the sensitivity of PHR data file. If they want to upload or update a PHR file, request send with descriptions to key issuer. Then the key issuer verifies the profile and send the one-time key to data owner for their persistence. And, also data owner manages the data users privilege access over the PHR data.

Multiple file partitioning technique

After data owner upload a PHR file the multiple file partitioning technique is used to partition the file based on sensitivity of data. The privileged based access structure is provided by data owners. The PHR files are partition into three files based on sensitivity of data. Fig 3 shows the partition types of sensitive PHR file.

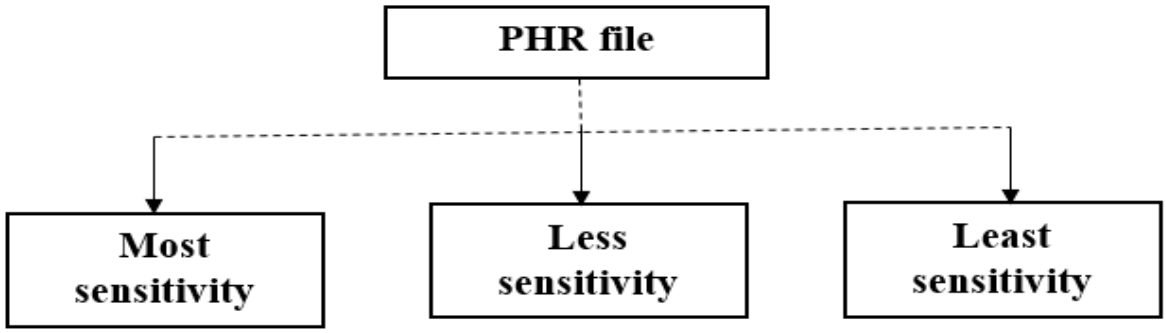


Fig 2 PHR file partitioning

Based on the privilege structure (Most sensitivity, less sensitivity, least sensitivity) data user get access over PHR files, well-defined privilege structure form based on the sensitivity of PHR and credential of data owners PHR file.

https://doi.org/10.37896/pd91.3/91341

ISSN: 0369-8963

ECC algorithm in our proposed model

To address the challenge of securing cloud computing data, the ECC algorithm opted for encryption technology. Elliptic Curve Cryptography is an asymmetric encryption technique that employs the algebraic structure of elliptic curves over finite fields to generate cryptographic keys that are faster, smaller, and more efficient. Rather than employing the traditional method of generating keys by multiplying very large prime numbers, ECC makes use of the properties of elliptic curve points and equations. Due to the fact that ECC helps to provide equal security with reduced computer and battery resource utilization, as well as robust key exchange characteristics.

In our proposed work, the partition files are encrypted using ECC algorithm, Encryption is used to get a confidentiality towards the PHR file. Figure 3 shows the flow of ECC encryption process.

PHR partition files are divided into 20bytes of individual blocks, then convert the PHR file into integer ASCII value. The ACSII values are map using Hash mapping of elliptic curve coordinate. Reverse mapping is used while decryption.

Choice the ECC curve i.e. $\boldsymbol{Y^2 = X^3 + X + 1 \bmod 23}$ (1)

Because it is impossible to discover the multiplicand without first knowing the elliptic curve's original and product points, the security of this type of encryption is dependent on the ability to perform a point multiplication (multiplicative inverse).The complexity of the task is determined by the size of the elliptic curve (prime value).

The elliptic curve $\mathbf{E_{23}(1, 1): y^2 = x^3 + x + 1}$ **over p = 23** (equation 1),for each X€{0...22},anintegerysuchthaty^{2}mod23=(x^3+x+1)mod23.Finite field E_p (a, b). Check the finite field is singular ($4a^2 + 27b^3 = 0$) or non-singular ($4a^2 + 27b^3 \neq 0$) if it's singular then choose another finite field of elliptic curve. After that choose the base point G (x, y) and find the order of G called Rank of G (n). Select the key randomly k, K € (0, n). Table1 shows the Y value coordinate value of the equation E23(1, 1): y2 = x3 + x + 1.

Table 1 Y values calculation

Y value	Y2	Y^2 Mod 23
0	0	0
1	1	1
2	4	4
3	9	9
4	16	5
5	25	3
6	36	3
7	49	5
8	64	9
9	81	4
10	100	1
11	121	6
12	144	6
13	169	8
14	196	12
15	225	18
16	256	3
17	289	13
18	324	2

 https://doi.org/10.37896/pd91.3/91341

ISSN: 0369-8963

19	361	16
20	400	9
21	441	4
22	484	1

Table 2 shows the X coordinate value of the equation E23(1, 1): y2 = x3 + x + 1

Table 2 X values calculation

X value	**$x^3 + x + 1$**	**X value mod 23**	**Y-value One**	**Y-value Two**
0	1	1	1	22
1	3	3	7	16
2	11	11	N/A	N/A
3	31	8	10	13
4	69	0	0	0
5	131	16	4	19
6	223	16	4	19
7	351	6	11	12
8	521	15	N/A	N/A
9	739	3	7	16
10	1011	22	N/A	N/A
11	1343	9	3	20
12	1741	16	4	19
13	2211	3	7	16
14	2759	22	N/A	N/A
15	3391	10	N/A	N/A
16	4113	19	N/A	N/A
17	4931	9	3	20
18	5851	9	3	20
19	6879	2	5	18
20	8021	17	N/A	N/A
21	9283	14	N/A	N/A
22	10671	22	N/A	N/A

Table 3 shows all the points E23(1, 1) as ordered pairs (x, y)

Table 3 Points of Elliptic curve

(0, 1)	(0, 22)	(1, 7)
(1, 16)	(3, 10)	(3, 13)
(4, 0)	(5, 4)	(5, 19)
(6, 4)	(6, 19)	(7, 11)
(7, 12)	(9, 7)	(9, 16)
(11, 3)	(11, 20)	(12, 4)

 https://doi.org/10.37896/pd91.3/91341

ISSN: 0369-8963

(12, 19)	(13, 7)	(13, 16)
(17, 3)	(17, 20)	(18, 3)
(18, 20)	(19, 5)	(19, 18)

G=(3, 10)onE_{23}(1,1)=> $y^2=x^3+x+1$, a=1, b =1
Find the points values plot in the graph and perform modular addition and multiplication using following formulae's,

$$\boldsymbol{\lambda = \frac{Yq-Yp}{Xq-Xp}\ mod\ p} \quad \text{and} \quad \boldsymbol{\lambda = \frac{3(X2g-a)}{2Yg}\ mod\ p}$$

$$\boldsymbol{Xr = (\lambda 2 - Xg - Xg)\ mod\ p} \quad \text{and}$$

$$\boldsymbol{Yr = (\lambda(Xg - Xr) - Yg)\ mod\ p}$$

1G=(3, 10), 2G= (7, 12), 3G = (19, 5), 4G = (17, 3), 5G = (9, 16), 6G = (12, 4), 7G = (11, 3), 8G= (13, 16), 9G = (0, 1), 10G = (6, 4), 11G = (18, 20), 12G = (5, 4), 13G = (1, 7), 14G = (4, 0), 15G = (1, 16), 16G = (5, 19), 17G = (18, 3), 18G = (6, 19), 19G = (0, 22), 20G = (13, 7), 21G = (11, 20), 22G=(12, 19), 23G = (9, 7), 24G = (17, 20), 25G = (19, 18), 26G = (7, 11), 27G = (3, 13). (2)

These are the calculated G values (Multiplicative inverses). A scatterplot of the elliptic curve group Ep (a, b) = E23 (1, 1) is shown in Figure 3. (Symmetric around 22.5).The graph contains 28 points (infinity not shown) of the equation $E_{23}(1, 1)$: $y^2 = x^3 + x + 1$. And the graph is,

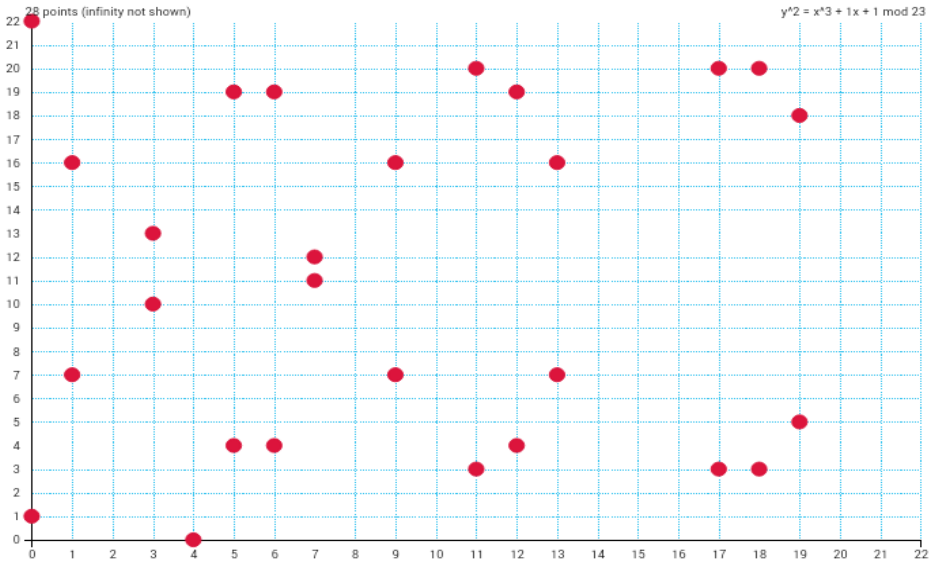


Fig 3 Scatterplot of elliptic curve group E_p (a, b) = E_{23} (1, 1)
(Symmetric around 22.5)

1G=(3, 10), 2G= (7, 12), 3G = (19, 5), 4G = (17, 3), 5G = (9, 16), 6G = (12, 4), 7G = (11, 3), 8G= (13, 16), 9G = (0, 1), 10G = (6, 4), 11G = (18, 20), 12G = (5, 4), 13G = (1, 7), 14G = (4, 0), 15G = (1, 16), 16G = (5, 19), 17G = (18, 3), 18G = (6, 19), 19G = (0, 22), 20G = (13, 7), 21G = (11, 20), 22G=(12, 19), 23G = (9, 7), 24G = (17, 20), 25G = (19, 18), 26G = (7, 11), 27G = (3, 13). These are the calculated G values (Multiplicative inverses).

https://doi.org/10.37896/pd91.3/91341

ISSN: 0369-8963

Calculate the public key based on the base point of the curve K=kG or $P_B=n_B$xG.
E_{23}(1,1)andG=(3, 10)andn_B=11,B'spublickeyis:
$P_B=n_B$xG = 11 * (3, 10) = 11G = (18, 20)
Select positive integer randomly (r), generate the ciphertext or encrypted text using the formulae,

$$C_m = rGP_m + rk_p \quad (3)$$

The encrypted text is stored in cloud server. The decryption process takes placed using the following formulae,
Encryption of P_M=(5, 4)forrandomkvalue,k=3.

$$P_m = C_m - K(rG)$$
$$= P_m + rKp - K(rG) \quad (4)$$
$$= P_m + rKG - KrG = P_m$$

C_M = {kG, P_m + kP_B} = {3*(3, 10), (5, 4) + 3*(18, 20))}
= {(19, 5), (7, 11)}

C_M = {(19, 5), (7, 11)}

P_M = C_M + kP_B– n_B(kG) = (7, 11) – 11*(3*(3, 10))
P_M =(5, 4)
Cipher text is converted into original form of PHR file for the use of data users' purpose. Data users access the decrypted file using a secret key provided by key issuer.

Cloud server

Servers that deliver cloud computing services in production are known as cloud servers. They used to store the PHRs encrypted file. The cloud server may read or manage the PHR file details using their user's name and password. If any unauthorized activity takes placed then the cloud server notifies the alert message to data owner and key issuer.

Key issuer

Key issuer verified the information and issue one-time secret keys for data user and data owner purposes. If data owner wants to upload or update the PHR file he/she give request to key issuer, then key issuer verify the data owner identity and provide key through mail. Data user needs to read or download a PHR file then give request to key issuer, then key issuer provide key based on the privilege based sensitive data structure. Key issuer blocks the unauthorized or unprivileged user try to access the PHR cloud. Always manage the access control of PHR cloud.

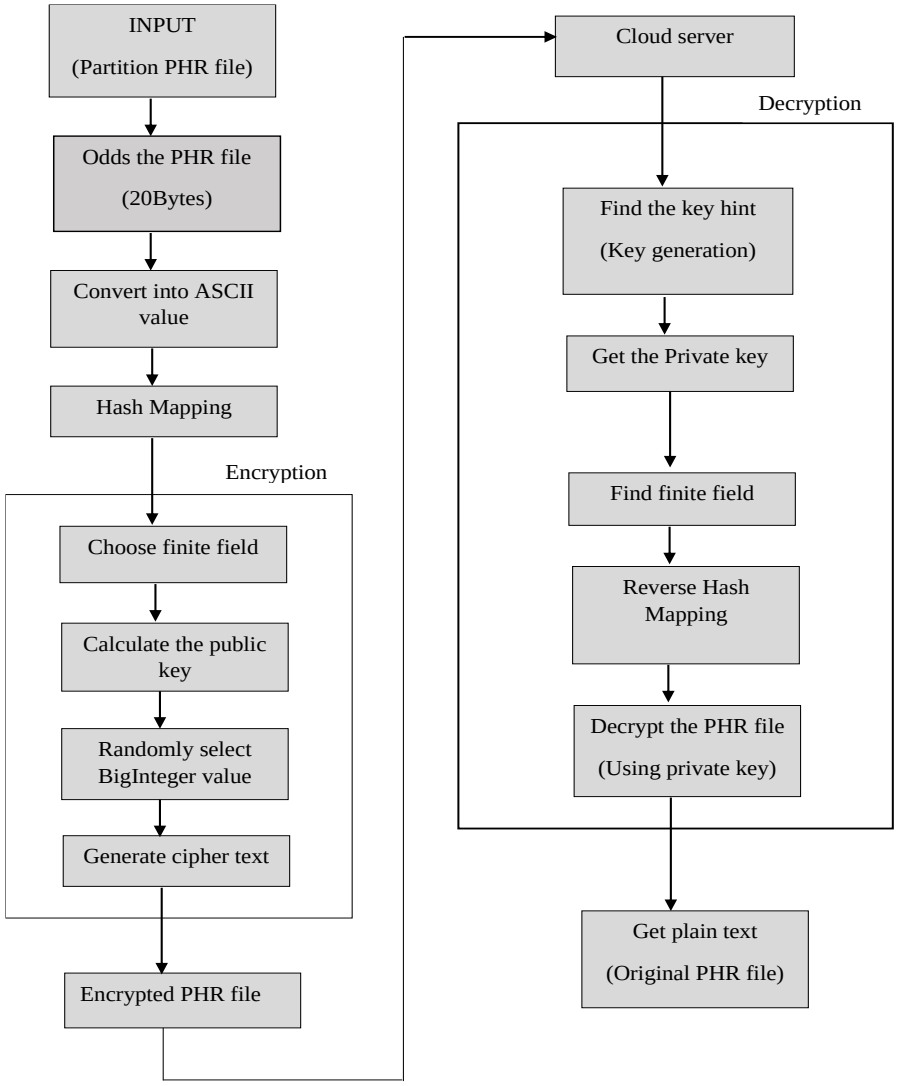
Data user

Users of personal health records (PHR) are those who receive exchange data from recipients and have some level of control or authorization over the processing of that data.If data user is a new user, he/she must register in the PHR system, or data user is already a registered user then login the PHR system with the use of username and password. Data user wants to access or download the PHR file then give request to key issuer. After giving request key issuer provide one-time secret key based on the privilege structure and sensitivity of data for their access and download action.

 https://doi.org/10.37896/pd91.3/91341

ISSN: 0369-8963

Fig 3 ECC encryption and decryption process in our proposed work



Implementation and Analysis

Our methodology's major objective is to develop a safe patient-centric paradigm while also providing effective key management. The key idea of our proposed model is partitioning the PHR file (most sensitive, less sensitive and least sensitive) according to the sensitivity of PHR file based on user privileges.

We use a set of data for each data owner registration and login, data user registration and login, patients' detail and attacker details (we perform some stimuli like unauthorized user) at least hundred set of data to perform the system configuration. The data owner registration contains their personal details like user name, password, owner name, hospital or organization name and address, owner's gender, date of birth, address, city, email address and mobile number. Data owner have the ability to upload a patient detail in cloud with certain privileges (user's access polices). After uploading the PHR file they partition based on the privileges. For example, patient medical summary (most sensitive PHR file) only accessed by doctors.

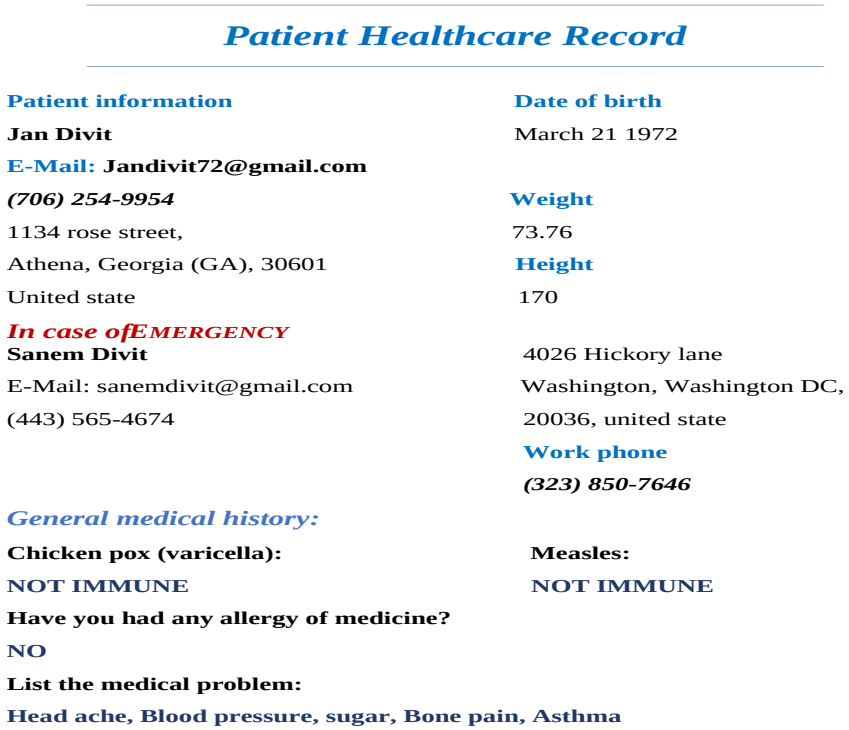
Most sensitive PHR's are patient's medical summary data, less sensitive PHR's are patient's medical report and least sensitive PHR's are patient's personal details. The privilege-based patient medical records are uploaded by data owner using the person in upload or upload the patients PHR in the format of word document, PDF, XPS document, open document, etc.,

 https://doi.org/10.37896/pd91.3/91341

ISSN: 0369-8963

Data owners are trusted and authorised representatives of each patient's Personal Health Record (PHR). Secret keys and access privileges for PHR users are managed using the ECC algorithm. In order to manage the access structure, the data owner must utilise a privilege-based framework that puts the patient's needs first.To self-protection the attributes of PHR's are encrypted by ECC algorithm. The write access is only given to data owners, for prevent the unauthorized contribution. The data access policies of our framework are flexible and allow the dynamic changes for certain emergency situations.

Fig. 4 shows the example PHR data set, this personal data set are uploaded by data owners. Patient's medical report consist of patients own physical and mental health data (information) such as patient id, diseases, symptoms, CT scan, blood test, blood pressure, pulse rate, blood sugar, doctor name etc., They are used by researches and doctors. Patient's medical report is used to provide correct perspective to patient's syndrome.



Patient Healthcare Record

Patient information
Jan Divit
E-Mail: Jandivit72@gmail.com
(706) 254-9954
1134 rose street,
Athena, Georgia (GA), 30601
United state

Date of birth
March 21 1972

Weight
73.76

Height
170

In case of EMERGENCY
Sanem Divit
E-Mail: sanemdivit@gmail.com
(443) 565-4674

4026 Hickory lane
Washington, Washington DC,
20036, united state

Work phone
(323) 850-7646

General medical history:

Chicken pox (varicella):
NOT IMMUNE

Measles:
NOT IMMUNE

Have you had any allergy of medicine?
NO

List the medical problem:
Head ache, Blood pressure, sugar, Bone pain, Asthma

Fig. 4 Example PHR data set

Fig. 5 shows the patient medical summary upload page, the patient's medical summary is uploaded by using patient ID, public key (provided by key issuer as per the data owner's request), medical summary and doctor name. Summary of data browse by device storage file (any format of file) and uploaded to cloud PHR.

https://doi.org/10.37896/pd91.3/91341

ISSN: 0369-8963

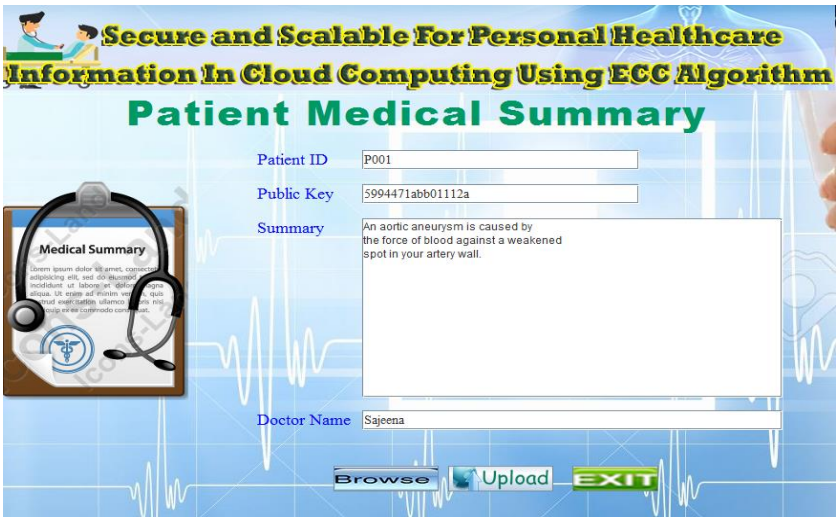


Fig. 5 Patient's medical summary uploaded page

Each partition files are encrypted aimed at to provide reliable confidentiality, we use ECC algorithm for both encryption and key generation. We provide two types of key, that is issued by key issuer for upload a PHR file (used by data owner) and view or download PHR file (used by data user).

The key will be generated by El-Gamal key generation algorithm. Data owner and data user want to upload and view or download PHR they give the key request with description to key issuer. Fig shows the data owner key request for uploading PHR in cloud. The page contains the fields like data owner, email address, mobile number and description is as shown in Fig. 6.

Fig. 6 Data owner key request page

Key issuer only maintains the key management and issue key based on the privileged-based structure. The complexity of key management is solved by ECC algorithm. Fig shows the data user key request page for view or download the PHR from cloud. The page contains the fields like data username, owner name of the PHR, attribute type (most sensitive, less sensitive, least sensitive), email address, mobile number and description for the clarification is shown in Fig. 7.

https://doi.org/10.37896/pd91.3/91341

ISSN: 0369-8963

Fig. 7 Data user key request page

After, sending request to key issuer. Key issuer performs the authentication and type of attribute and description. If the data owner or data user is authorized person then send the key through Email to the correspondent email address.

Fig. 8 shows the data user access of PHR using a secret key (private key) provided by key issuer. The secret is used to view or download the PHR file from cloud. Data user only accessed the PHR file based on the sensitivity of data. Key issuer only provides the key based on the user privilege access structure. So, the unauthorized users are easily recognized and notified to data owner to give the secure confidential framework.

Fig. 8 Data user access of PHR

The key is generated by key issuer using a master key. Size of master key is 128 bits (maximum size of key). Master key generated the key with different value in each time. Example key of ECC algorithm:

256-bit ECC private key:

0x51897b64e85c3f714bba707e867914295a1377a7463a9dae8ea6a18b91246319

256-bit ECC public key:

0x02f54ba86dc1ccb5bed0224d23f01ed87e4a443c47fc690d7797a13d41d2340e1

The key length is minimized (comprised) by encoding the key. After encoding the key size is 64-bit key for example

Minimized key: 65fjbd480gd33yvq

Fig. 9 shows the data user access PHR file using the private key provided by key issuer. If data user or unauthorized user tries to access over the privileges of PHR file, key issuer notices the party and block the user after three attempts of failure. Key issuer always has the access control to the cloud of PHR. We created PHR database in MySQL to store all the login, registration, login attempt, attacks data. The database has to use by the administrator (key issuer). Fully trusted entities only access the PHR file, the PHR files are encrypted and stored in cloud like unintelligible format. Here, the bellow format is decrypted PHR file of P001 patient personal details.

https://doi.org/10.37896/pd91.3/91341

ISSN: 0369-8963

S=)(#V□Kì¡²l½¡æIL°□³]¿>I□¦ìòbvë□□©Â□«òè¬~æ»
6äîTrî¿|3<¨ÓÏg
ðä!Fw1¤ «ZÐÌp+(åØ¹ÐJÚ9¯□ÿ□'OXëQ|ûnâ©Üg<÷!wzìÇé□b=

Fig. 9 Decrypted data of P001 patient personal record

The decrypted PHR's are stored shared by cloud. Cloud is used to exchange the PHR in the patient-centric model. ECC provide good reliable sharing communication between data owner, data user and key issuer. In contrast to the well-known RSA, ECC is a strong cryptography. RSA-like security with a reduced key size is possible with it. To maintain security, the size of the encryption key must be lowered using sophisticated operations since there are numerous resources accessible to break the encrypted keys. As a result, ECC safeguards administrator-user communications in this manner. As a result, it may be used to address issues such as processing overhead.

ECC employs the curves over the finite field to construct a secret that only the private key holder can reveal. The amount of times an ECC curve's equation was dotted makes it difficult to determine how many junction points there were. The ECC key is also a significant investment. RSA's 3072-bit key length is equivalent to ECC's 256-bit key length, ensuring the same level of security while using a smaller key.

These keys may be highly beneficial for devices that have a limited amount of processing capacity if they can be reduced in size.

ECC algorithm provides a highly secure communication (patient-centric model), data integrity and authentication with non-reputation communication and data confidentiality. Authentication, key generation and encryption of data provide confidentiality. In the perfect fact of ECC's secure key exchange capability, encryption with curve points and authentication pursuit the confidentiality of our proposed framework.

Result and Analysis

Analysis of confidentiality

Confidentiality refers to protecting data (PHR information) from being accessed by unauthorized users or unauthorized parties. Fig. 10 shows the analysis of confidentiality between existing and proposed system. It clearly shows that when compare with existing system, number of files increases the confidentiality also increases in our proposed system due to the strong encryption algorithm and better key management.

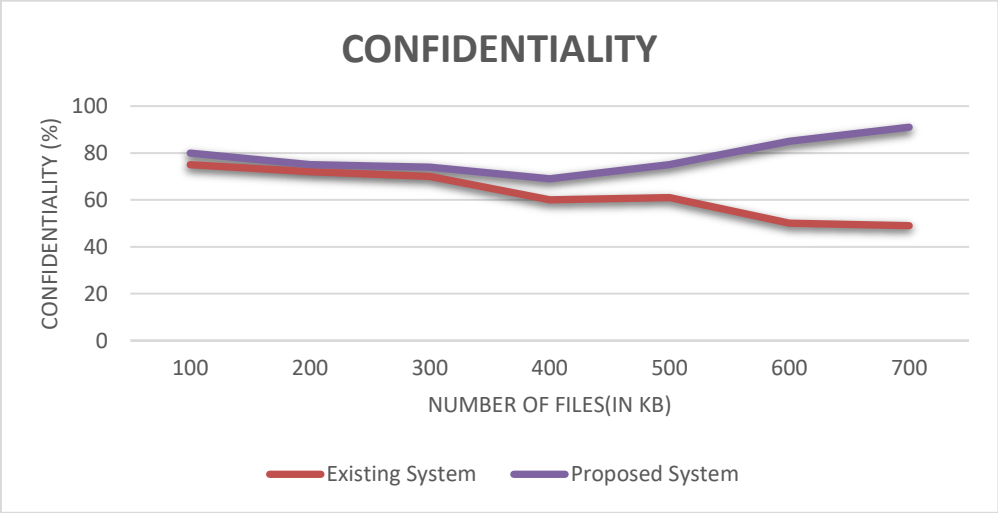


Fig. 10 Analysis of confidentiality

https://doi.org/10.37896/pd91.3/91341

ISSN: 0369-8963

Analysis of integrity

Information integrity relates to ensuring that information is not changed (altered) and that the source of the information is legitimate. Fig. 11 show the analysis of integrity between existing and proposed system. It evidently displays that when compare with existing system, number of files increases the integrity also get increases in our proposed system owed to the secure privilege access structure and unauthorized attack prevention.

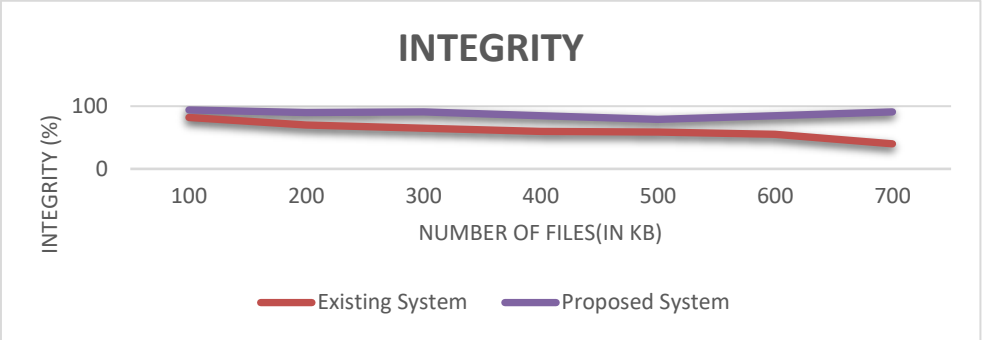


Fig. 11 Analysis of Integrity

Analysis of availability

Our proposed work provides highly secure availability, and verify if the information is accessible by authorized users or not. Fig. 12 shows the analysis of availability between existing and proposed system. It undoubtedly shows that when compare with existing system, number of files increases the availability also get increases due to the robust confidentiality and integrity.

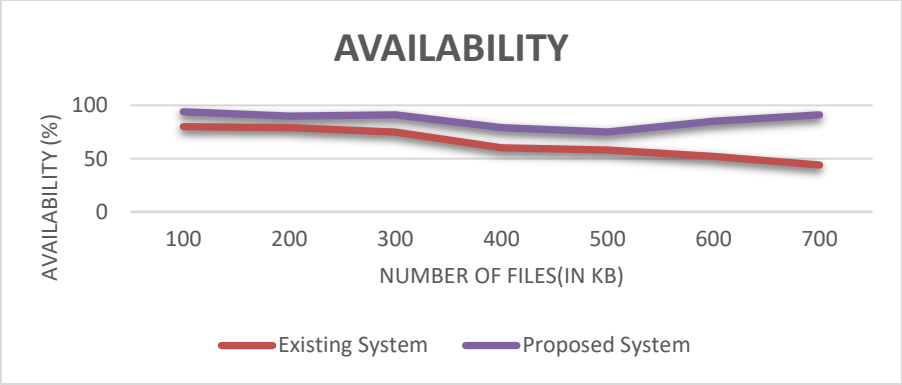


Fig. 12 Analysis of availability

Security and privacy

System files and data are safeguarded by the proposed scheme's combination of rules, controls, processes, and technology. Fig. 13 depicts the comparison of security and privacy between the current system and the proposed solution.It visibly shows that when compare with existing system, number of files increases the security and privacy also get increases due to the good security concern, key administration and stout encryption algorithm. To guarantee the control of other access to information (PHR files) about our data is privacy that is provided by projected system.

https://doi.org/10.37896/pd91.3/91341

ISSN: 0369-8963

Fig. 13 Analysis of security and privacy

Conclusion

PHR files are used to stored and shared in the cloud. Since security is the major concern in PHR, a new security based secure and scalable ECC algorithm is proposed which also uses privilege-based access structure and key issuer for key management. Privilege-based structure partition the PHR data files into different segments based on data sensitivity. Each segment of the PHR file is then shared to data users depends on data user privileges using a key provided by key issuer. In the scheme formally secure against unauthorized attacks. The proposed work performance is compared with exiting schemes, it's signifyingly reduce the computational complexity with minimizing storage space and provide good security over our own PHR files. Hence, it improves security further prevent unauthorized attacks and key management.

References

[1] Ming Li, Shucheg Yu and Kui Ren, "Securing Personal Healthcare Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner settings" Springer Security and privacy in communication networks, Vol. 50, No. 50, 2010, pp.89-106.

[2] VeerrajuGampala, SrilakshmiInuganti, and Satish Muppid "Data Security in Cloud Computing with Elliptic Curve Cryptography" International Journal of Soft Computing and Engineering (IJSCE), Vol. 2, July 2012, pp. 139-141.

[3] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and 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, Jan 2013, pp. 131-143.

[4] Alowolodu O. D, Adetunmbl A. O, and Ogundele O. S "Elliptic Curve Cryptography for Ssecuring Cloud Computing Applications" International Journal of Computer Applications, Vol. 66, No. 23, March 2013, pp. 0975-8887.

 https://doi.org/10.37896/pd91.3/91341

ISSN: 0369-8963

[5] U. Jyothi., K. Nagi Reddy., B. Ravi Prasad "Review of achieving secure, scalable fine-grained data access control in cloud computing" International Journal of Engineering and Computer Science Vol. 2, No.8, Aug 2013, pp. 2440-2447.

[6] Rakesh & Vardhan **"**Sharing of personal health records in cloud computing" International Journal of Engineering Applications, Vol. 3, No. 6, Nov-Dec 2013, pp. 1769-1773.

[7] D. Sangeetha, Vaidehi Vijayakumar, ValliammaiThirunavukkarasu, and Aiswarya Ramesh "Enhanced Security of PHR System in Cloud Using Prioritized Level Based Encryption" Springer-Verlag Berlin Heidelberg, Vol. 20, No. 59, 2014, pp. 57-69.

[8] FatosXhafa, Jianglang Feng, Yinghui Zhang, Xiaofeng Chen, and Jin Li "Privacy-Aware Attribute-Based PHR Sharing with User Accountability in Cloud Computing" Springer Journal of supercomputing, Vol. 71, No. 5, 2015, pp. 1607-1619.

[9] Pradeep Deshmukh "Design of cloud security in PHR for Indian Healthcare services" Computer and Information Sciences, Journal of King Saud University, Jan 2016, pp.281-287.

[10] Leyou Zhang, Qing Wu, Yi Mu and, Jingxia Zhang "Privacy-Preserving and Secure Sharing of PHR in the Cloud" Springer Systems-Level Quality Improvement, Vol. 40, Sept 2016, pp.13-267.

[11] Joseph K. Liu, Man Ho Au, Xinyi Huang, Rongxing Lu, Jin Li "Fine-grained Two-factor Access Control for Web-based Cloud Computing Services", IEEE Transactions on Information Forensics and Security, Vol.2, Jan 2017, pp. 484-497.

[12] R. JosephiusArunkuma, and R. Anbuselvi "Enhancement of Cloud Computing Security in Health Care Sector" International Journal of Computer Science and Mobile Computing, Vol. 6, No. 8, Aug 2017, pp. 23 – 31.

[13] E. Zaghloul, T. Li, and J. Ren, "An attribute-based distributed data sharing scheme" IEEE Global Communication, Vol.57, Dec 2018, pp. 2595-2608.

[14] Sanaa Sharaf and Nidal F. Shilbayeh "A secure G-cloud-based framework for government healthcare service" IEEE Transactions and content mining, Vol. 7, Mar 2019, pp. 37881.

[15] Puja M Tambe, and Prof. Nisar S Shaikh "A Review Paper on Privacy Based Secure Sharing of PHR in the Cloud using Encryption" International Journal of Engineering Research & Technology (IJERT), Vol. 8, No. 12, Dec 2019, pp. 887-890.

 https://doi.org/10.37896/pd91.3/91341