Modified Elliptic Curve Cryptography Model for Personal Health Record Sharing in Cloud with Trust Valuation

ChudamanDevidasrao Sukte[1], Dr. Emmanuel. M[2] and Dr. Ratnadeep R. Deshmukh[3]
[1]Dept. of Computer Science & I.T,
Dr. B. A. M. University, Aurangabad, India.

[2]Department of IT
P.I.C.T, Pune, India
[3]Dept. of Computer Science & I.T,
Dr. B. A. M. University, Aurangabad, India.

Abstract:

In this research work, a novel SSPHR (Secure Sharing PHR) methodology based on Modified Elliptic Curve Cryptography (MEEC) with Trust Evaluation based RE-encryption key is introduced for securely sharing the Personal Health Records (PHR) of the patients via cloud. The patients being the owners of his/her PHRs initially register within the cloud, and upload their PHR onto the cloud. Before uploading the PHR documents, the owner (patients) encrypts the data using a newly proposed Modified Elliptic Curve Cryptography (MEEC) model. Whenever, a cloud user (may be a doctor, insurance person, family members, pharmacist or research scholar) request for the access of the patients' encrypted PHR to edit or view his/her records, the owner (patient) alone can grants permission. Based on the functionality (role played in the society) of the user, the PHR owner grants certain level of access only after re-encrypting it based on the trust evaluation. This level of access granted to various categories of users is de-fined in the Access Control List (ACL) by the PHR owner. More particularly, the PHR user performs aTrust Evaluation to verify whether the user is a direct user (already existing users) or indirect user (Authorized sources like friend's company). This proposed model permits the PHR owners to exercise complete control over their PHR.

Keywords

PHR; Cloud Storage; Secure Sharing; Modified Elliptic Curve Cryptography (MEEC); Trusted Evaluation based RE-encryption key

1. Introduction

Cloud computing has evolved as a critical computing platform for providing ubiquitous access to a wide variety of resources such as 'hardware, software, infrastructure, and storage'. As a result, the cloud computing architecture favors organizations' through relieving them the time-consuming task of infrastructural development and encouraging them to rely on 3rd party Information Technology (IT) services [9]. Furthermore, the cloud computing approach offers undeniable potential to improve the collaboration amongst numerous aid players, and to ensure the continual access on public health data and quantity capability [10] [11] [15] [21]. A PHR paradigm enables a patient to generate, administer, and manage medical data with one central location using online technologies, making storage resources, retrieving, and exchange extremely effective [16] [17] [18]. Although it is simple to provide PHR access to anyone and everyone, there seem to be a number of security and privacy issues that might impede adoption. It is critical to have a precise "data access control" that operates with non-trusted servers to ensure users' (patients') private management of their own PHRs [19] [20].

Before storing data on the cloud, it is a fantastic strategy to encrypt it. Essentially, the PHR owner is required to choose how to encrypt data and who has accessible on it [22] [23] [24]. A PHR records document can only be accessed by users who have been provided the decryption key, whereas the rest of the customers must stay private. Allowing each user to get keys from the owner whose PHR wishes would restrict access if the patients aren't constantly in online [25] [26].

Another option is to hire centralized capabilities to resolve all of the key management for all PHR owners; however this demands more confidence in an authority.Attempts have been made to investigate a PHR system with more PHR providers and tenants. Patients may well be the proprietors, with complete authority of their own PHR information, such as the ability to construct/generate, manage, and remove information. All the owners' PHRs are stored on the server that belonging to the PHR service provider. A friend, a guardian, or a researcher, for example, could be one of the customers. Users try to read or write to someone's PHR records through the server if they have access to multiple owners' data at the same time [27] [28]. The two major security objectives or concerns for any electronic health record paradigm are "user-controlled read-write access and revocation". In the PHR system, user controlled writes access control prevents the unauthorized users from accessing and altering records. b) Access Control on Finer Scale Distinct users must be permitted to read different sets

Manuscript received January 5, 2022
Manuscript revised January 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.1.78

of documents; therefore “fine-grained access” control should be employed [29].

The major contribution of this research work is:

- Introduces a Modified Elliptic Curve Cryptography (MEEC) model to encrypt the PHR with high level of security including new Trust Evaluation based RE-encryption key to validate whether the user is a direct or indirect user.

The rest of this paper is organized as: section II discusses the literature works undergone in PHR privacy preservation in cloud. Section III tells about the proposed SSPHR methodology: an overview. In addition, modified ECC based encryption with trust based re-encryption is discussed in Section IV. The results acquired with the proposed work are discussed comprehensively in Section V. This paper is concluded in Section VI.

2.Literature review

In 2019, Florence *et al*. [1] to ensure data security, authors have explored a novel technique based on “searchable attribute” based encryption, and have named it as user based encryption. They undergo a comprehensive security study to ensure that their suggested model outperforms current techniques in terms of information and ciphering costs. In 2019, Suresh *et al.* [2] User Usage Based Encryption (UUBE), based on the searchable encryption method has been proposed as a unique diversified access control framework. Each enciphered event has been connected to a set of credentials by a data owner/proprietor. In 2020, Chen *et al.* [3] have developed a safe searchable encryption technique for searching on encrypted personal health records stored inside a “NoSQL database” on “semi-trusted cloud servers”. And most query operations accessible in plaintext database systems have been supported by the suggested technique, including “multi-dimensional, multi-keyword searches” with range queries. An Adelson-Velsky Landis (AVL) tree has been used to establish the index throughout the developed framework, and an Order-Revealing Encryption (ORE) technique has been employed to encrypt the AVL tree and perform queries. In 2018, Zhang *et al.* [4] for diagnostic improvements in e-Health systems, a BSPP method has been proposed. The suggested protocol would satisfy the specific objectives, as per the information security. In addition, the authors have investigated the efficiency of the control method using JUICE. In 2018, Sujansky*et al.* [5] has proposed a standard-based paradigm for the automatic gathering of patient information via personal medical equipment, and the secure sharing of that data with approved physicians' Electronic Health Records (EHRs). The paradigm offered a framework of standardized assessments created by the Continua Alliance and has applied in a range of business solutioms for the automatic collection of information from patients' individual health equipment.

3.Proposed SSPHR methodology: An Overview

In this research work, we take into account a PHR infrastructure with numerous PHR users and owners. Patients who have complete authority of their own PHR data, i.e. one who can generate, modify, and remove it, are referred to as owners. All of the owners' PHRs are stored on a central server, owned by the PHR service provider. Users can be anyone; a colleague, a caretaker, or a researcher, for instance. Users can access PHR documents via the server to read or write to someone's PHR, and a single user can have access to multiple owners' data at the same time.

3.1 Requirements

The key requirement of “patient-centric” PHR dissemination is that every patient has the specification about who has the accessibility to their personal PHR information.

The following is an overview of the scalability and reliability prerequisites:

- The security of information: Unauthorized persons (along with the server) who haven't had sufficient attributes that fulfill the access rules or who do not have sufficient key access privileges should never be able to decode a PHR document, especially if they are operating together. Distinct customers should indeed be permitted to see different sets of documents, therefore fine-grained access control should be implemented.
- Revocation on demand: Whenever a customer's attribute expires, the user must no longer be able to view the subsequent PHR files with that attribute. The related security feature is forward secrecy, which would be commonly referred to user revocation. There's also user revocation, which removes all the user's access rights.
- Control of write access: Illegal contributors are not capable of writing the proprietors' PHRs, and only the genuine contributors will be able to view the server with responsibility.
- Data access regulations might be adaptable, allowing for dynamic modifications to established restrictions. PHRs, in particular, should be available in times of emergency.
- Durability, efficiency, and usefulness are all important factors. Individuals from personal and public realms should be supported by the PHR system.

- In order to enjoy accessibility, the proprietors' efforts in managing users and keys must be minimized.

3.2. Overview of the proposed Work

The health-care environment has grown to the cost-effective and simple interchange of PHRs among the many e-Health network collaborators. However, placing private health information on cloud storage threatens it to disclosure or theft, necessitating the development of techniques that ensure PHR privacy.

This paper focuses on providing a novel cloud-based SSPHR approach. Both forward and backward access restriction are enforced in the proposed SSPHR approach. Inside the suggested method, there have been two categories of PHR users: "(a) patients or PHR owners, and (b) PHR users who are not owners, but can be a health insurance company, physicians, researcher, family members or friends of patients, pharmacists or doctors". Patients as PHR owners are allowed to upload the encrypted PHRs to the cloud by allowing users access to certain parts of the PHRs. In this research, the PHR of the data owners is encrypted using a novel MEEC. The data will be encrypted and saved on the cloud. The PHR owners provide each person in the user group of the later type to access the PHRs up to a particular extent, based on the role of the user. The PHR owner defines the levels of access given to eachusers in the ACL. The owner may, for example, grant complete access to the PHRs, particularly to the patients' close relatives or acquaintances. Similarly, insurance company representatives may have only accessibility to sections of PHRs holding details concerning health insurance claims, but other sensitive health information, such as the patient's medical history, may well be prohibited for these kind of users. RE-encryption key is issued to the user based on the Trust Evaluation to validate whether they are a direct or indirect user. Therefore, the patient can also exert total control over their PHRs and revoke accessibility permissions using this method.

Step 1: Initially, the PHR owner registers within the cloud. This phase is manifested in Fig.1.

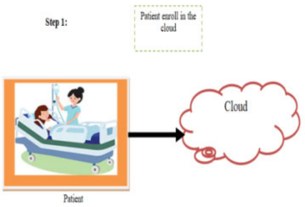

Fig 1. Patient enrolls in the cloud

Step 2: Once, the PHR owner has been registered, he/she uploads their encrypted PHR records within the cloud. The original PGR records are encrypted via the newly introduced MECC model.

This phase is illustrated in Fig.2.

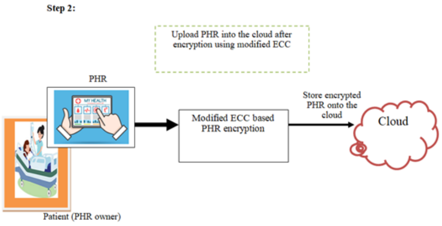
Step 2:
Upload PHR into the cloud after encryption using modified ECC
PHR
Modified ECC based PHR encryption
Store encrypted PHR onto the cloud
Cloud
Patient (PHR owner)

Fig 2. PHR owner uploads his/her medical records in the cloud

Step 3: When a user (for example: friend of the patient, a doctor, pharmacist and insurance person) request access for the PHR of the patient, the PHR owner validates their access level to his/her records. This access level varies from user to user and these access levels are defined in the ACL. As per our illustration, the friend of the patient and doctor will be given complete control to access the PHR, while the pharmacist will be permitted only to view the prescribed medicines and not the history or personal details of the patients. On the other hand, the insurance person will be permitted to access the personal information and the overall summary of the PHR alone. This phase is shown diagrammatically in Fig.3.

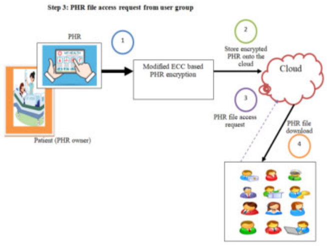
Step 3: PHR file access request from user group
PHR
1
Modified ECC based PHR encryption
2
Store encrypted PHR onto the cloud
Cloud
3
PHR file access request
PHR file download
4
Patient (PHR owner)

Fig 3. Access Request by diverse users

Step 4: In prior to permitting the users to decrypt the records based on their access level, a trust evaluation is made by the PHR owner. This trust evaluation is accomplished via the newly proposed. As per this Trust Evaluation based RE-encryption key model, the PHR owner validates, whether the user is a direct user or an indirect user. The direct users are those, who are already having the access rights (i..e existing users),whereas, the indirect user are authorized sources (may be a friend's company). Finally, the users can decrypt the PHR and access it. This phase is shown in Fig.4.

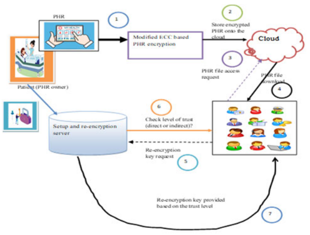
PHR
1
Modified ECC based PHR encryption
2
Store encrypted PHR onto the cloud
Cloud
3
PHR file access request
PHR file download
4
Patient (PHR owner)
Setup and re-encryption server
6
Check level of trust (direct or indirect)?
Re-encryption key request
5
Re-encryption key provided based on the trust level
7

Fig 4. Trust based Re-Encruption model for data re-encyption

3.3 Preliminaries

Patients or PHR owners may govern access to patient information using the suggested technique, which ensures fine-grained access control [4]. Patients upload encrypted PHRs by individually encrypting the partitions of PHRs, such as “(i) personal information, (ii) medical information, (iii) insurance-related information, and (iv) prescription information”, according to the suggested methodology. Furthermore, the PHR client programmed produces the re-encryption settings, which would then be communicated towards the Setup And Re-Encryption Server (SRS). If an user requests particular part of the PHR, they must authenticate and then retrieve it from the cloud. It is worth mentioning that the client can't decrypt the Health records at this time, since the client must get the necessary decryption settings from the SRS. The SRS examines the asking recipient's ACL to see whether the PHR administrator have authorized the user access to the segment in which the decryption specifications have been sought. The SRS should create the right variables and transmit them to the specific user based on the access rights provided in the ACL. It's worth mentioning that perhaps the objective of this research is confined to safeguarding the PHR. Furthermore, common protocols like as IPSec or SSL are anticipated to be used to protect interaction between the customer and SRS. The protocols mentioned above have been extensively used on the Internet and therefore are effective for safeguarding communications. Communication security. SRS is in charge of the setup, key generation, and re-encryption stages.

Access to PHR: Only authorised individuals should have access to PHR's sensitive information, as per the proprietors. PHR operations may also be transferred to a third providers to save the expense of constructing and operating PHR centres. Holders of information, on the other hand, are wary of such companies. In reality, because of the great value of private data, these outsourced party servers may engage in harmful activity to disclose PHR, such as the well-known instance reported in [13]. In some cases, however, the practical need of saving people's lives must take precedence above security issues. As a consequence, an ideal encryption algorithm for the proprietors must meet the criteria listed below. – Protect the privacy of sensitive data. – Deliver PHR information with fine-grained access restriction.

In the actual world, an attacker could use the recipient's characteristics to get sensitive data (Fig. 5). If any of the characteristics include”XX hospital, medicine, treatment cycle, cancer,” for example, an attacker can infer that the recipient is a doctor. As a result, a significant challenge in actual situations is how to safeguard user personally identifiable information in an ABE. Anonymous ABE (AABE) is indeed a type of Identity-Based Encryption (IBE) that is supplied anonymously. The recipient's identity is hidden by the ciphertext in such a scenario. “Boneh and Franklin” [14] proposed the first anonymous IBE system. The ciphertexts in anonymous encrypted algorithm cannot expose the access policy that is used to encrypt communications.

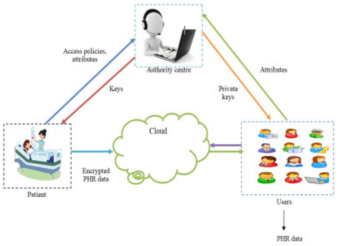

Fig 5. Acess Encrypted PHR in Cloud

The private keys corresponding to the user's characteristics are used to decrypt the received ciphertexts. The user can successfully decrypt the ciphertext if the characteristics of the private keys match to those of the access policy. The user would be unable to obtain anything if that's not the case. Therefore in such situation, a user should execute all decryption processes to get the information. He or she checks to see whether he or she is the intended recipient. The decryption algorithm can then be used to retrieve the information. All of these result in substantial reception overhead, particularly in resource-constrained networks.

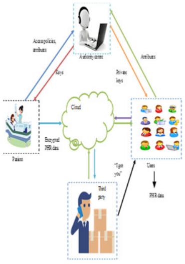

Fig 6. Attribute leakage to third party

3.4 Entities

Three entities have been involved in the proposedwork for sharing PHRs within the cloud architecture: “(a) the cloud, (b) the SRS, and (c) the users”. The following is a brief description of each of the entities.

- The Cloud: The system suggests that PHR owners to store their records in the cloud enabling future secure sharing with the other customers. Users upload and download PHRs to / from cloud storage, which also are deemed to become an untrustworthy entity. As the cloud resources are solely used to upload and download PHRs, no modifications towards the cloud are required.
- For the system's users, the SRS is a “semi-trusted server” that would be in charge of generating public/private key combinations. The SRS additionally produces re-encryption keys for secured PHR exchange amongst users. SRS has been regarded as a semi-trusted entity

throughout the suggested technique. Although the SRS keeps track on the keys, the PHR information is not reveled to them. The users are in charge of encryption and decryption. The SRS not only manages keys, but it also controls full access to information. The SRS is indeed a stand-alone server which can be placed on a public cloud owing to the cloud's lack of trustworthiness. For the patients' convenience, the SRS might be administered either by a trustworthy third-party organisation or a consortium of institutions. It could also be sustained by a group of patients who are linked together.

- Due to the engagement of health professionals and/or patient self-control over SRS, SRS managed by hospitals or by a group of patients would inspire higher confidence. (a) Patients (proprietors of PHRs who wish to safely exchange them with others) (b) family members or friends of patients, physiciams and physicians, representative of insurance companies, chemists, and academics are the two main categories of components in the network. Friends or family members have been considered private domain users inside the suggested method, whereas all other users are regards the public domain users. The PHR proprietors can grant users of both the private and public domains with varying levels of access to the PHRs. Individuals throughout the private domain, for example, could have full access to the PHR, but customers throughout the public domain, includingdoctors, academics, and pharmacies, may only have accessibility to only certain parts of the PHR. Furthermore, if the PHR owner deems it necessary, the abovementioned individuals may well be granted complete access to the PHRs. To put it in another way, the suggested technique enables patients to have fine-grained access control over their PHRs. To access the SRS's services, all users must enroll with the SRS. The enrollment process is based on the users' functions, such as doctor, researcher, or pharmacist.

The PHR Partitioning: "Insurance-related information ,Personal information and prescription information, medical information" are divided into four sectioms in the PHR. It is worth mentioning that the above-mentioned division is just not rigid. The user can split the PHR into few or even more divisions with his or her choice. PHRs may be easily split as well as expressed in many forms, such as XML. Furthermore, the PHR administrator can provide the equivalent degree of authentication to several partitions. Certain of the PHR components may well be prohibited to the user, and also some users may not be permitted complete access to healthcare data. A chemist, for example, may also have accessibility to prescription and insurance information, but not to personal or medical data. Similarly, complete accessibility towards the PHR may well be granted to family/friends. A researcher may simply require access to medical data in order to de-identify patients' personal information. The PHR owner determines the access privileges to distinct PHR partitions, which are then sent to the SRS when the information is uploaded to the cloud.

4. Modiifed ECC based Encryption with Trust based Re-encryption

4.1 MECC based encryption

The ECC model being the Public-Key encryption algorithm provides better security than the RSA model. But, the exiting ECC model is not applicable for current multimedia usage. Therefore, we have introduced a new MECC model for safe-guarding the multimedia applications. The patient record is encrypted using the modified ECC. on a curve , the MECC is centered using a prime number function with certain base points, and it is utilized as a maximal limit.

$$Y^2 = X^3 + uX + v \tag{1}$$

Here, u,v are the integers.

In MECC, three key sets are generated.

(a)Public key α_k

(b)private key β_k

(c)secrete key δ_k

- Primarily, α_k is generated as to server and it is encrypted.
- Then, β_k is generated on the server side and it is decrypted.
- Thirdly, δ_k is generated as α_k and β_k and point on the curve P_c.

The secrete key is multiplied in encryption and divided in decryption phase. β_k is picked from N number of values arbitrarily, and α_k is generated using β_k and P_c. Mathematically, α_k is shown in Eq. (2).

$$\alpha_k = \beta_k + P_c \tag{2}$$

Secrete key δ_k **:** it is computed from the total of α_k , β_k and P_c. This is mathematically shown in Eq.(3).

$$\delta_k = \alpha_k + \beta_k + P_c \tag{3}$$

Encryption; the transformation of the original PHR data D into affine points takes place on the curve. Subsequently, the acquired data are encrypted. It contains two cipher texts $Ec(t_1)$ and $Ec(t_2)$ shown in Eq. (4) and Eq. (5), respectively.

$$Ec(t_1) = \frac{K * P_c}{\delta_k} \tag{4}$$

$$Ec(t_2) = \frac{[D + (K * \alpha_k)]}{\delta_k} \tag{5}$$

In addition, K denotes the random number generated between 1 to $n-1$.

Proposed Trust based Re-encryption Process: The re-encryption key management will distribute the key to the users to decrypt the data. The key will be provided based on the trust values of the users. The trust value of the user can be collected from the data owners. This is mathematically shown in Eq.(6).

$$T_v = (r, S_m, S_B) \tag{6}$$

Here, r, S_m, S_B points to the successful interactions, user management failure and user behavior failure.

$$T_v = \varpi(r, S_m + S_B) \tag{7}$$

The trust will be of two types:

(a) Direct trust- The already existing users can access the PHR of the patient, based on his/her permitted accessibility.

(b) Indirect trust- Authorized sources like friend's company can be permitted to access the data, and here too the restriction of accessibility of records do exist. Once, the user's trust level is validated, the decryption takes place.

Decryption: The decryption process is done using secret key δ_k and private key β_k. This is mathematically shown in Eq.(8).

$$D = \delta_k \ (Ec(t_2)) \text{-} (Ec(t_1)) \ \beta_k \tag{8}$$

5.Results and discussions

5.1 Simulation Procedure

The improved EEC-based SSPHR was developed in JAVA/Cloudsim, and the results within each investigation were evaluated. "https://catalog.data.gov/km/dataset/va-personal-health-record-sample-data" provided the dataset for assessment. Furthermore, the modified ECC method was compared against Blowfish [30], RSA [30], AES [30] , El-Gamal [31], ECC , and modified El-Gamal [32] in terms of "key processing time, encryption time, and decryption time". The assessment of time consumption was accomplished with flow sizes of 100, 200, 300, and 400.

5.2 Analysis on Time Consumption

The time required for Key generation time of the Proposed Modified ECC is compared over the existing models like Blowfish, RSA, AES, El-Gamal, ECC, and modified El-Gamal. This evaluation is undergone by varying the file size from 100, 200, 300 and 400, respectively. Under all the variations in the file size, the proposed model had achieved the least key generation time (in ms). Among all the variation in the file sizes, the most littleKey generation time as 1ms, when the file size is 100, 200 and 300. In addition, the Decryption time (ns) of the proposed as well as existing model is shown in Table II. On observing the outcomes, the MECC had achieved the least Decryption time (ns) under all the variation in the File Size. When the File Size=100, the MECC had achieved the least Encryption time (ns) as 58ms, which is the better than Blowfish=6152, RSA=3174, AES=1256, El-Gamal=1061, ECC=429 and Modified El-Gamal=377. The decryption time (ns) of the proposed and mixing model is manifested in Table III. The decryption time (ns) of the MECC had achieved the least value for every variation in the File Size. The Turn Around Time(ns) of the proposed as well as existing model is manifested in Table IV. Under all variation in the File Size, the MECC had achieved the least Turn Around Time(ns). When the File Size=400, the Turn Around Time(ns) of the MECC is 268, which is the least score while compared to Blowfish=36195, RSA=14613, AES=10751, El-Gamal=7329, ECC=3319, and modified El-Gamal=1446. Thus, from the overall evaluation, it is vivid that the MECC had achieved the least Key generation time, Decryption time (ns), Encryption time (ns) and Turn Around Time(ns), respectively.

Table 1. Analysis on key generation time (in ns)

File Size	Blowfish [30]	RSA [30]	AES [30]	El-Gamal [31]	ECC	Modified El-Gamal [32]	Modified ECC
100	11	7	5	2	1	1	1
200	12	9	6	3	2	2	1
300	13	11	7	4	2	2	1
400	15	12	9	5	3	2	2

Table 2. Analysis on Encryption time (in ns)

File Size	Blowfish [30]	RSA [30]	AES [30]	El-Gamal [31]	ECC	Modified El-Gamal [32]	Modified ECC
100	6152	3174	1256	1061	429	377	58
200	8751	4656	2334	1701	996	432	169
300	15025	6944	4549	2467	1707	545	173
400	27614	9007	5531	5237	1876	722	180

Table 3. Analysis on Decryption time (in ns)

File Size	Blow fish [30]	RSA [30]	AES [30]	El-Gamal [31]	ECC	Modified El-Gamal [32]	Modified ECC
100	3000	1253	1006	782	425	374	56
200	5834	2449	1604	940	504	428	62
300	6587	4726	2337	1367	950	540	70
400	8566	5594	5211	2087	1440	722	86

Table 4. Analysis on Overall turn around time (in ns)

	Blow fish [30]	RSA [30]	AES [30]	El-Gamal [31]	ECC	Modified El-Gamal [32]	Modified ECC
100	9163	4434	2267	1845	855	752	115
200	14597	7114	3944	2644	1502	862	232
300	21625	11681	6893	3838	2659	1087	244
400	36195	14613	10751	7329	3319	1446	268

5.3 Analysis on Cipher Text Attack

Table V shows the results of a cypher text attack evaluation between the modified ECC encryption model and the traditional models. In this research, the key breakage time by cipher text attack has been determined, and the performance of the suggested cryptosystem has been compared to existing models. Moreover, the modified ECC encryption model for key size (64 bits) attains the highest key breakage time (912200ns) , which is better than Blowfish=36100, RSA=257900, AES=339000, El-Gamal=650000 and Modified El-Gamal=683690. This demonstrates the PHR's security using the suggested crypto scheme. The system's security against a cipher text attack with a longer key breakage time is demonstrated by looking at the table.

Table 5. Analysis on Cipher text attack

Key size (bits)	Blow fish [30]	RSA [30]	AES [30]	El-Gamal [31]	ECC	Modified El-Gamal [32]	Modified ECC
64	36100	257900	339000	650000	661450	683690	912200
128	106600	327900	412600	757100	810100	832950	1083493
192	127000	742600	1444200	2172600	2531200	2789920	3075466
256	129200	840800	1445100	2203100	2661050	2809970	3443796

5.4 Comparitive Analysis on Brute force attack

Table VI shows a comparison of the modified ECC encryption model to traditional methods when it comes to Brute Force attacks. This research determines the key breakage time by brute force assault, as well as the performance of the proposed cryptosystem compared to existing models. Furthermore, the modified ECC encryption model for key size 128 bits attains the highest key breakage time of 2182946 msand the existing schemes models had attained the breakage time as Blowfish=99600, RSA=263200, AES=369000, El-Gamal=471100, ECC=805800 and Modified El-Gamal=1.99 Xe^{06}.

Table 6. Analysis on Brute force attack

Key size (bits)	Blow fish [30]	RSA [30]	AES [30]	El-Gamal [31]	ECC	Modified El-Gamal [32]	Modified ECC
64	44000	223900	261200	428100	466700	474100	581500
128	**99600**	263200	**369000**	471100	805800	1.99 Xe^{06}	2182946
192	104700	495100	1155300	1314800	3840100	4305400	4989033
256	200100	503800	1232200	8622100	9138150	1.01 Xe^{07}	11250436

6.Conclusion

This paper had proposed a novel SSPHR methodology based on MEEC with Trusted Evaluation based RE-encryption key for securely sharing the PHR of the patients via cloud. Once, the user registers within the cloud, he/she stores their own encrypted PHR records within the cloud. This encryption was carried out using the MECC model. Whenever, a cloud user (may be a doctor, insurance person, family members, pharmacist or research scholar) request for the access of the patients' encrypted PHR to edit or view his/her records, the owner (patient) alone can grants permission. Based on the functionality (role played in the society) of the user, the PHR owner granted certain level of access only after re-encrypting it. The re-encryption has been carried out using the newly developed Trusted Evaluation based RE-encryption key. This Trusted Evaluation based RE-encryption key aids in finding the functionality of the user (whether a direct or indirect one). Finally, the proposed work has been compared over the existing models in terms of Brute Force attacks, Key generation time, Decryption time (ns), Encryption time (ns) and Turn Around Time (ns), respectively. When the File Size=400, the Turn Around Time (ns) of the MECC is 268, which is the least score while compared to Blowfish=36195, RSA=14613, AES=10751, El-Gamal=7329, ECC=3319, and modified El-Gamal=1446.

References

[1] M. Lilly Florence & Dhina Suresh , "Enhanced secure sharing of PHR's in cloud using user usage based attribute based encryption and signature with keyword search", Cluster Computing,2019

[2] Dhina Suresh & M. Lilly Florence ,"Securing Personal Health Record System in Cloud Using User Usage Based Encryption", Journal of Medical Systems, 2019

[3] Lanxiang Chen, Nan Zhang, Hung-Min Sun, Chin-Chen Chang, Shui Yu & Kim-Kwang Raymond Choo,"Secure search for encrypted personal health records from big data NoSQL databases in cloud", Computing volume, 2020

[4] Aiqing Zhang & Xiaodong Lin ,"Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain", Journal of Medical Systems,2018

[5] Walter Sujansky & Douglas Kunz,"A standard-based model for the sharing of patient-generated health information with electronic health records", Personal and Ubiquitous Computing, 2018

[6] Parsa Sarosh,Shabir A. Parah,Khan Muhammad,"Secret Sharing-based Personal Health Records Management for the Internet of Health Things", Sustainable Cities and Society,2021

[7] Chaitanya Singh,Deepika Chauhan,Ranjan Walia,"Medi-Block record: Secure data sharing using block chain technology",Informatics in Medicine Unlocked,2021

[8] Pengfei Liang,Leyou Zhang,Juan Ren,"Privacy-preserving decentralized ABE for secure sharing of personal health records in cloud storage",Journal of Information Security and Applications,2019

[9] F. Deng, Y. Wang, L. Peng, H. Xiong, J. Geng and Z. Qin, "Ciphertext-Policy Attribute-Based Signcryption With Verifiable Outsourced Designcryption for Sharing Personal Health Records," IEEE *Access*, vol. 6, pp. 39473-39486, 2018. doi: 10.1109/ACCESS.2018.2843778

[10] M. M. Madine *et al.*, "Fully Decentralized Multi-Party Consent Management for Secure Sharing of Patient Health Records," IEEE *Access*, vol. 8, pp. 225777-225791, 2020. doi: 10.1109/ACCESS.2020.3045048

[11] S. Wang, D. Zhang and Y. Zhang, "Blockchain-Based Personal Health Records Sharing Scheme With Data Integrity Verifiable," IEEE *Access*, vol. 7, pp. 102887-102901, 2019. doi: 10.1109/ACCESS.2019.2931531

[12] J. Wei, X. Chen, X. Huang, X. Hu and W. Susilo, "RS-HABE: Revocable-storage and Hierarchical Attribute-based Access Scheme for Secure Sharing of e-Health Records in Public Cloud," IEEE *Transactio*ms *on Dependable and Secure Computing*. doi: 10.1109/TDSC.2019.2947920

[13] M. Li, S. Yu, Y. Zheng, K. Ren and W. Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," IEEE *Transactio*ms *on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131-143, Jan. 2013. doi: 10.1109/TPDS.2012.97

[14] M. Ali, A. Abbas, M. U. S. Khan and S. U. Khan, "SeSPHR: A Methodology for Secure Sharing of Personal Health Records in the Cloud," IEEE *Transactio*ms *on Cloud Computing*, vol. 9, no. 1, pp. 347-359, 1 Jan.-March 2021. doi: 10.1109/TCC.2018.2854790

[15] Y. Zhang, D. He, M. S. Obaidat, P. Vijayakumar and K. -F. Hsiao, "Efficient Identity-Based Distributed Decryption Scheme for Electronic Personal Health Record Sharing System," IEEE *Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 384-395, Feb. 2021. doi: 10.1109/JSAC.2020.3020656

[16] S. Bao, M. Chen and G. Yang, "A Method of Signal Scrambling to Secure Data Storage for Healthcare Applications," IEEE *Journal of Biomedical and Health Informatics*, vol. 21, no. 6, pp. 1487-1494, Nov. 2017. doi: 10.1109/JBHI.2017.2679979

[17] L. Zhang, W. You and Y. Mu, "Secure Outsourced Attribute-based Sharing Framework for Lightweight Devices in Smart Health Systems," IEEE *Transactio*ms *on Services Computing*. doi: 10.1109/TSC.2021.3073740

[18] Q. Feng, D. He, H. Wang, L. Zhou and K. R. Choo, "Lightweight Collaborative Authentication With Key Protection for Smart Electronic Health Record System," IEEE *Sensors Journal*, vol. 20, no. 4, pp. 2181-2196, 15 Feb.15, 2020. doi: 10.1109/JSEN.2019.2949717

[19] M. M. Madine *et al.*, "Blockchain for Giving Patients Control Over Their Medical Records," IEEE *Access*, vol. 8, pp. 193102-193115, 2020. doi: 10.1109/ACCESS.2020.3032553

[20] Z. Ying, L. Wei, Q. Li, X. Liu and J. Cui, "A Lightweight Policy Preserving EHR Sharing Scheme in the Cloud," IEEE *Access*, vol. 6, pp. 53698-53708, 2018. doi: 10.1109/ACCESS.2018.2871170

[21] K. Liang and W. Susilo, "Searchable Attribute-Based Mechanism With Efficient Data Sharing for Secure Cloud Storage," IEEE *Transactio*ms *on Information Forensics and Security*, vol. 10, no. 9, pp. 1981-1992, Sept. 2015. doi: 10.1109/TIFS.2015.2442215

[22] L. Xu *et al.*, "ASBKS: Towards attribute set based keyword search over encrypted personal health records," IEEE *Transactio*ms *on Dependable and Secure Computing*. doi: 10.1109/TDSC.2020.2970928

[23] K. Edemacu, B. Jang and J. W. Kim, "Efficient and Expressive Access Control With Revocation for Privacy of PHR Based on OBDD Access Structure," IEEE *Access*, vol. 8, pp. 18546-18557, 2020. doi: 10.1109/ACCESS.2020.2968078

[24] W. Li *et al.*, "Unified Fine-Grained Access Control for Personal Health Records in Cloud Computing," IEEE *Journal of Biomedical and Health Informatics*, vol. 23, no. 3, pp. 1278-1289, May 2019. doi: 10.1109/JBHI.2018.2850304

[25] S. Fugkeaw, "A Lightweight Policy Update Scheme for Outsourced Personal Health Records Sharing," IEEE *Access*, vol. 9, pp. 54862-54871, 2021. doi: 10.1109/ACCESS.2021.3071150

[26] Q. Li, Y. Zhang, T. Zhang, H. Huang, Y. He and J. Xiong, "HTAC: Fine-Grained Policy-Hiding and Traceable Access Control in mHealth," IEEE *Access*, vol. 8, pp. 123430-123439, 2020. doi: 10.1109/ACCESS.2020.3004897

[27] C. -T. Li, D. -H. Shih, C. -C. Wang, C. -L. Chen and C. -C. Lee, "A Blockchain Based Data Aggregation and Group Authentication Scheme for Electronic Medical System," IEEE *Access*, vol. 8, pp. 173904-173917, 2020. doi: 10.1109/ACCESS.2020.3025898

[28] D. Froelicher, J. R. Troncoso-Pastoriza, J. S. Sousa and J. Hubaux, "Drynx: Decentralized, Secure, Verifiable System for Statistical Queries and Machine Learning on Distributed Datasets," IEEE *Transactio*ms *on Information Forensics and Security*, vol. 15, pp. 3035-3050, 2020. doi: 10.1109/TIFS.2020.2976612

[29] M. A. Uddin, A. Stranieri, I. Gondal and V. Balasubramanian, "Continuous Patient Monitoring With a Patient Centric Agent: A Block Architecture," IEEE *Access*, vol. 6, pp. 32700-32726, 2018. doi: 10.1109/ACCESS.2018.2846779

[30] Priyadarshini Patil, Prashant Narayankar, Meena S.M., "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish",Procedia Computer Science,vol. 78, pp. 617-624, 2016.

[31] M. Ali, A. Abbas, U. Khan and S. U. Khan, "SeSPHR: A Methodology for Secure Sharing of Personal Health Records in the Cloud," IEEE Transactions on Cloud Computing, doi: 10.1109/TCC.2018.2854790.

[32] Chudaman Sukte, “Efficient Cryptographic Protocol Design for Secure Sharing of Personal health Records in Cloud”, in communication

Chudaman Devidasrao Sukte, Research scholar, Department of Computer Science and Information Technology, Dr Babasaheb Ambedkar Marathwada University Aurangabad, India. He published more than 10 research papers in reputed Journals conferences. His area of research includes Cloud computing, Grid Computing.

Dr. Emmanuel Mark, BE(CSE), MTech(CSE), PhD(CSE) working as Professor, Information Technology Department, Pune Institute of Computer Technology, Pune, India. He is BOS IT, Savitribai Phule Pune University. He published more than 50 research papers in reputed Journals conferences. He has 21 years of teaching and industrial experience. His area of research includes Cloud computing, Database, Big Data and Medical Image Processing.

Professor (Dr.) R. R. Deshmukh, M.E., M.Sc. (CSE) Ph.D. FIETE, PEIN Fellow, Working As Professor, Department of CSIT, Dr. B.A.M. University, Aurangabad, (MS), India. Coordinator of DST-FIST program, University Coordinator, MHRD GIAN program, Chairman, IETE Aurangabad Centre 2014–2018, Organized Zonal ISF-2016, Sectional President, ICT Section ISCA-2019, Life member ISCA, CSI, ISTE, IEEE, IAEng, CSTA, IDES, ACEE. Management Council, Senate, Academic Council Member at University, Edited Twelve books, published more than 235 research papers in reputed Journals, Editor-In-Chief, CSI Journal of Computing. Visited Russia, USA, China, Spain, Philippines, Uzbekistan, Thailand for academic work. He can be reached at rrdeshmukh.csit@bamu.ac.in