Original Research Article

J. Computing & Int. Systems (2022) 309–316

Journal of Computing and Intelligent Systems

Journal homepage: www.shcpub.edu.in

ISSN: 2456-9496

DATA SECURITY IN CLOUD COMPUTING WITH ELLIPTIC CURVE CRYPTOGRAPHY AND MULTI-FACTOR AUTHENTICATION

S. Meena[#1], P. Madhubala[#2]

Received on 12 NOV 2022, Accepted on 07 DEC 2022

Abstract — In recent years, cloud computing-based health data maintenance and sharing it through the cloud has become an effective platform to healthcare sector. Health experts can give medical service by getting health data on any device in anywhere at any time. The significant challenge faced by a healthcare institute is secure sharing of Personal Health Records (PHR) in cloud among general practitioner, medical services, scan centers, testing labs, insurance firms and etc. Due to cloud maintenance is done by third parties, if the intruders attacked PHR, it can create consequential problems because it contains many important data such as clinical decisions, health conditions, drug usage, and etc. To overcome this problem, security of sensitive PHR is accomplished with encryption techniques. In this paper, the Personal Health Records (PHR) are encrypted by using elliptic curve cryptography mechanism to obtain confidentiality and integrity of health data while transmitting through the cloud. In addition, multi-factor authentication techniques has been applied to authenticate the users before provide the data accessing permission. The experimental outcomes demonstrate better performance in terms of file encryption and decryption time, file uploading and downloading time, key generation time and all. It also allows secure sharing of PHR over cloud by defending against internal and external threats

Keywords - Cloud Computing, Cloud Security, Personal Health Records, Elliptic Curve Cryptography (ECC), Encryption, Decryption, Multi-factor Authentication

I. INTRODUCTION

In emerging technologies, many organizations and service sectors are using cloud computing Pancholi et al. (2016) for storing and accessing their data. Particularly, healthcare sector is widely adopting towards cloud storage to store and access Dang, L et al. (2019) patient health information, doctors' details, treatment procedures, admission details and other sensitive information for further proceedings and to handle patient's health effectively. Cloud computing is offering different services Li, Jin et al (2017) - Li et al (2017) called software-as-a-service (SaaS), platform-as-a-services (PaaS), security-as-a Service (SECaaS) and infrastructure-as-a-services (IaaS) to the service requesters. Numerous volumes of information have been stored and retrieved from a different location with these services. Because of cloud offering SECaaS Li, Jin et al (2018) to the requester, many people use the cloud service to store and access their Personal Health Records (PHR) Rao et al (2017). While there are many benefits and security measures for using the cloud, there are various challenges in fully securing sensitive data, especially when using third-party servers on the Internet. Also, cloud lacks visibility, limited data control, participants in malicious attacks, incomplete control over access to sensitive data, limited data monitoring, inability to control internal attacks and regulatory compliance Zhang et al (2016) -Thwin et al (2018) when accessing data on third-party cloud servers. This cloud computing risk is overcome by various mitigation processes such as the DevSecOps process Kumar et al (2020), centralized management service providers with integrated security Song et al (2016) automated application deployment and management tool Maes et al (2018). The DevSecOps process constantly improves the code quality to minimize vulnerabilities and improve data access speeds. An automated application deployment and management tool integrates various security measures to reduce security threats. Finally, many tools are managed in a centralized management process to minimize intermediate access to the cloud environment. Mitigation techniques try to avoid intermediate access and internal attacks and maintain important data security, reliability, privacy, agility and scalability, but cloud security remains a significant challenge Xiong et al (2018) - Liu et al (2015). Shared PHR data is compromised by different criteria such as identity management, data theft, user authentication, internal subordination, infected usage, external intrusion and data integrity. These factors are the reasons for data privacy and security issues in the cloud environment. Therefore, cloud security is managed using various encryption techniques Shabir et al (2016), Dhote et al (2016), such as re-encryption, attribute-based encryption (APE), key-based approach, ciphertext policy encryption, identity-based encryption, and expressive key encryption. Hierarchical attribute encryption, proxy re-encryption, and fuzzy identity-based encryption.

* Corresponding author: E-mail: [1]smeenamphil@gmail.com, [2]madhubalasivaji@gmail.com

[1]Research Scholar (Part-Time), Department of Computer Science, Periiyar University, Salem.

[2] Research Supervisor, Department of Computer Science, Don Bosco College, Dharmapuri, India.

Dhote et al (2016), such as re-encryption, attribute-based encryption (APE), key-based approach, ciphertext policy encryption, identity-based encryption, and expressive key encryption. Hierarchical attribute encryption, proxy re-encryption, and fuzzy identity-based encryption. Although these techniques successfully manage data security, keys that are easily predictable by the intermediate user are generally shared. Therefore, data security, privacy, authentication and confidentiality still exist when sharing and accessing data in the cloud. In this work, encryption techniques are integrated with biometric authentication techniques Kakkad et al (2019), Joseph et al (2020) to deal with cloud security and privacy issues. During this process, a multi-factor authentication method [20] is used to authenticate user information. The authentication process works with encryption algorithms; therefore, the prediction of shared keys is difficult to access by unauthorized users. Furthermore, biometric technique is used to authenticate the user before granting access permission and improving user authentication. At last, the shared data is stored in encrypted form done by Elliptical Curve Cryptography (ECC). The encrypted data storage process enhances the overall data privacy, confidentiality and security features. Eventually, the performance of the system is evaluated using experimental results and discussion. The remaining manuscript is arranged as follows; Section 2 analyzes the latest techniques for maintaining data security. Section 3 discusses the working process of PHR data security based on multi-factor authentication and the excellence of the system evaluated in Section 4. Summary of the paper discussed in Section 5.

II. RELATED WORKS

(Ramesh, D., and L., 2017) Applying of e-stream cipher and dynamic update policy to create secure data storage process in cloud environment. The e-stream cipher encryption and encryption process was used to maintain sensitive data security when sharing data in the cloud. Apart from these, the Dynamic Merkel Hash B+ Tree Algorithm (TMHD) is a secure short signature used to manage data integrity. The two methods discussed ensure a minimum computation complexity when providing security for sensitive data in a cloud environment.

(Masala GL et al., 2018) Introduces biometric techniques to manage data security in the cloud. This process ensures data security in two words: authorizing the user before granting access and securing the data before storing it on a third-party server. User authentication is done using the fingerprint biometric authentication process, which is done in the OpenStack framework. Data is stored according to the fragmentation concept. Integration of the biometric and encryption algorithm solves key sharing in cloud and authentication process problems.

(Suresh, D. et al., 2019) Developing a user-related encryption process for securing PHR data in the cloud. For each event, the application is planned as credentials used to maintain data privacy in the cloud. The credential information applies during the data access process, and many credentials are used to establish data confidentiality. This process, which considers usage and user credentials, is a private key that is difficult for the intermediate user to access. For each event, user credentials are constantly changed; therefore, data privacy, integrity and confidentiality are successfully maintained.

(Doshi N. et al., 2019) Maintaining PHR data security and privacy in the cloud server using Cybertext Policy-Attribute Based Encryption (CB-APE). This encryption algorithm uses a variety of functions such as user access delegations, utilization revocations, encrypted files probing, accountability, and multi-authority processes to establish security for sensitive data shared in the cloud.

(Subramaniam et al., 2020) Applying the elliptic curve Diffie-Hellman Crypto Process (EDHCP) to manage security in a big data cloud environment. This method effectively encrypts the data with minimum complexity. Successful generation of the key leads to a reduction in encryption and encryption time with minimal computational overhead. This method ensures 70% better performance compared to existing encryption techniques.

(Prabhu Kavin et al., 2020) Implements cloud security using different encryption algorithms, such as elliptical cryptography (ECC), access control, and lightweight digital signature (LDSA). Initially, the ECC algorithm is used to generate keys integrated with the access control mechanism to control access to user data. The LDSA approach is used to maintain data integrity when accessing and sharing data in a cloud environment.

(Meddah N. et al., 2018) Creates a secure cloud-based PHR data sharing process using Lightweight Attributes with Access Control Encryption techniques (LAACE). The data is stored in the cloud by establishing access control and confidentiality, which is done with the elliptic curve integrated encryption algorithm. The key policy attribute-based encryption algorithm ensures access control of shared data. The policy-based access process avoids intermediate attacks, minimizes collusion and guarantees data confidentiality. According to various researchers, data security plays an important role when sharing data in a cloud environment. Many techniques, encryption methods and biometric procedures are used to manage data security. Often, however, shared data is accessed by an intermediate and unauthorized user. This causes the trust between the service provider and requester. Also, reduces data privacy, confidentiality, authentication and authorization. Therefore, this paper is concentrated on biometric techniques integrated encryption system to improve the overall data security of the cloud environment. The detailed working process of the introduced algorithm is explained in the following section.

III.PRESERVING DATA SECURITY USING ELLIPTIC CURVE CRYPTOGRAPHY AND MULTI-FACTOR AUTHENTICATION

This section describes how PHR data security works by using elliptic curve cryptography and multi-factor authentication.

Cryptography in Cloud Computing

A common method in computer networks for ensuring the security of data and communications sent over the network is cryptography. The sender's plain text message is

converted into a specific form called "cypher text" and encrypted before being transmitted across the network. The encrypted text communication is decoded at the receiver's end into the original plain text using a straightforward decryption process. Therefore, the encoded message can only be decoded by the communication's sender and receiver. To address network security challenges, cryptography is used. The information is confidential, and no unapproved individuals, businesses, or procedures have access to it or have been made aware of it.

The phrases are distinct even if they are related to privacy. Confidentiality, on the other hand, is a component of privacy that makes it possible to shield data from unauthorized users. (ii) Data integrity is the general consistency, precision, and fullness of the data. No matter how long or how frequently it has been viewed, information kept in a database will be comprehensive, accurate, and dependable if the integrity of the data is safe. Data security ensures that information is protected from outside influences. (iii) Availability denotes that data must be accessible when required. This necessitates the proper operation of the computer systems used to store and process the information, as well as the security measures needed to keep it safe and the communication channels used to access it. In order to avoid service interruptions brought on by power outages, hardware malfunctions, and system updates, highly available systems aspire to be available at all times. Preventing service denial attacks, such as a flood of incoming messages that effectively force the target system to shut down, is one way to ensure availability. (iv) A person's intention to uphold their end of a contract is referred to as non-repudiation. This means that neither one of the parties to a transaction may deny receiving a transaction, and vice versa. (v) The process of verifying a user's identification is called authentication. This method connects incoming requests to credentials for identification.

A. Multi Factor Authentication in Cloud Computing

MFA is now even more essential in light of the rise of cloud computing. They can no longer think of a user as a physical security threat on the same network once the healthcare sectors move their systems to the cloud. To make sure that persons who access computers are not criminals, further security measures should be put in place. Since users can access these systems from anywhere at any time, MFA can assist them in verifying their identity by requesting extra authentication factors that are more challenging for hackers to duplicate or crack using brute force techniques. The MFA system is based on one of three extra sorts of data.

- Things you are aware of, like a PIN or password
  - Things that you own, like a badge or smartphone
  - Things that are inherent in you, like voice recognition or a biometric like fingerprints
  - Various MFA Styles
  - Based on place

Risk-based authentication, also known as adaptive Authentication Answers to PSFs, passwords, and OTPs are considered knowledge factors in MFA and can be either possessed or known. OTPs generated by smart phone apps, sent through mail or text, access badges, USB devices, smart cards or fobs, security keys, software tokens, and certificates are possession factors. Factors of inheritance: behavior analysis, facial recognition, voice, iris, retina, and other biometrics. Location-based MFA often examines the user's geolocation and, if available, IP address. When authenticating, adaptive authentication considers extra characteristics while also considering context and behavior. It frequently uses these values to determine the amount of risk associated with a login attempt.

PHR Maintenance Using ECC and Biometric Integrated Multi Factor Authentication

This process uses biometric features integrated multi factor authentication method to manage data integrity. During the data sharing process, the PHR data is stored in the encrypted form, for preserving data confidentiality and privacy. Also, the data can be accessed only after verifying the user; this process manages the user authentication and authorization process. According to the discussion, the detailed working process of PHR data security is illustrated in Fig 1. Data security is installed on the health center and user side. Initially, the PHR owner encrypts the data using the Elliptic Curve Cryptography (ECC) approach and stored on the cloud server. The user will access the data by authenticating themselves using a multi-factor authentication mechanism integrated with the biometric feature. This process ensures data security, confidentiality, integrity and authentication

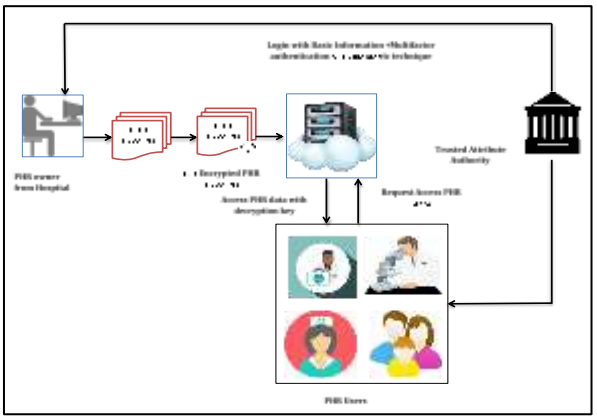


Fig. 1 Preserving Data Security Using Elliptic Curve Cryptography and Multi-Factor Authentication Process

Encrypting Personal Health Records (PHR)

The first step in this process is to encrypt personal health records before storing them in the cloud server. This encryption process is done using the Elliptic Curve Cryptography (ECC) approach. The PHR log encryption process minimizes intermediate attacks and

Unauthorized access and manages data security.

Initially, a public and private key pair must be created for the data owner and the server. The generated keys are shared between the owner-server pair using the ECC approach. Data is encrypted and decrypted to access PHR data from the cloud server. Here, the input PHR data is divided into different blocks; the secrete Key S_k is generated for each block, which is stored is

in the cloud. During the data access process, whole blocks are collected and merged to access the original PHR Data.

Key initialization

The first step in this task is to create the public key (PK) and the primary secret key (MSK).The Central Authority (C.A.) then selects the largest prime number(p), and the bilinear group $(G, G1)$ is formed with the order p. Then the generator$g \in G$, $y \in Z_p$, $h \in G$, $t_{ij} \in Z_p (i \in [1,n], j[1,n])$. Then CA computes the $T_{ij} = g^{t_{ij}} (i \in [1,n], j \in [1,n_i])$ and $Y = e(g,h)^y$. According to this concept, the PK and MSK are initialized as follows.

$$\begin{cases} PK = \left(e, g, h, Y, T_{ij} (i \in [1,n], j[1,n_i])\right) \\ MSK = \left(y, t_{ij} (i \in [1,n], j \in [1,n_i)\right) \end{cases} \quad (1)$$

In above eqn (1), p is a large number of prime numbers from that Z_p the group is formed. Two different hash functions are denoted as t and t' that is mapped with the group Z_p as,

$$Z_p \rightarrow \{0,1\}^* * \{0,1\}^* \quad (2)$$

The two universal hash functions t and t' is acknowledged to a Central Authority (C.A.)

Key Sharing

The generated key must then be shared with the owner and the server. This key sharing process performed via the C.A. For each user u, the attribute list L is maintained with MSK. From there, the secrete key is generated using eqn (3).

$$SK_L = \left\{h^{y+r}, \forall v_{i,j} \in LD_{i,j} = \left(T_{i,j}\right)^r, g^r, L\right\} \quad (3)$$

In eqn (3), $r \in Z_p$, possible attributes are denoted as $v_{i,j}$, generated key is denoted as $D_{i,j}$. The key generated in Eqn (3) shares the PHR data between the owner and the user, enabling the encryption and decryption process.

PHR Data Encryption using ECC

After sharing the generated key, the shared PHR data is encrypted using a pair of keys such as public (encryption) and secret key (decryption). The data encryption process ensures the privacy, confidentiality and integrity of the data. In this process, the sender receiver knows the public key(G^d), and d is the receiver's private key. From the key value, the sender generates a new value (y) called G^y. This process is used to compute the symmetric key performed by the key generation function eqn (4).

$$k = K(G^{dy}) \quad (4)$$

Eqn (4) K is referred to as the key generation function. This encryption process is done between the data owner and the user; therefore, elliptic curve parameters are generated before the encryption process is completed. Hence, each user must create a pair of keys, such as the public key (Q) and the private key(d). According to Eqn (5), the public key Q is formed.

$$Q = dG \quad (5)$$

Here, G is referred to as the curve generator. Refers to the sender (PHR owner) key (d_A, Q_A) and the receiver key(d_B, Q_B). In ECC, messages are denoted by points (x, y) and the encryption process is performed according to eqn (6).

$$Q_B = d_A d_B G = d_B d_A G = d_B G \quad (6)$$

In addition to this, PHR data is encrypted according to the Data Encryption Key (D.K.), which is Eqn (7).

$$CT = (A, E = Enc_{DK}(M)) \quad (7)$$

In eqn (7), C.T. is represented as ciphertext of the message, A is the attribute access structure, M is the PHR data. The effective generation of the key leads to minimizing overheads and communication cost.

Authenticating user to Access Health Records

The Shared PHR data is accessed anywhere by the user by authenticating themselves to avoid security issues. User authentication is done with a biometric integrated multi-factor authentication process. Initially, the user registers their details with the respective website to authorize the user to access the data. This process involves contextual recognition, which includes I.P. Address details, date, geo location and time. This information authenticates user contextual information, and authorizes changes of user information by sending a one-time password to the users. After completing the initial verification, a biometric process is performed to authorize the user to improve the user authentication process. Here, ear biometric features are used to authenticate the user because ear biometric information contains a huge range of specific and unique features that help identify users. Also, after 70 years the ear features changed, which affects the security systems and detects the person more accurate. For these reasons, ear biometric features are used to successfully authenticate and authorize user information.

Ear Biometric Authentication Process

Initially, the collected ear biometric features are converted from color images to a grayscale image to reduce time usage; it also helps predict the exact ear features. The RGB

color of the ear images is converted to grayscale images by estimating the weighted average value of the red, green and blue values. The color change of the image is done using eqn (8).

$$GS = 0.2989 * Intensity(r) + 0.58701 * Intensity\ (g) + 0.1140 * Intensity\ (b) \quad (8)$$

After changing the ear image color representation, the noise of the biometric feature should be removed to improve the user identification process. In this work, median filters are used to replace the noise-affected pixels. Median filter effectively removes unwanted pixels without affecting image quality and edge. Each pixel in the image is compared with the neighboring pixels, and if the pixel value is changed or distorted, it will be replaced by computing the median values. The pixels are arranged in order, and the middle pixel is selected to replace the distorted pixel. The feature or description is extracted from the noise-removed ear image. This task is accomplished through rapid section analysis with key point detection, orientation assessment and descriptor extraction. The primary step is point detection because most key points belong to the description used to authenticate the user when accessing PHR data. During this process, a corner approach is used to explore the key points where the 16 pixel circle is used. The 16 pixels are named clockwise to identify the edges of the ear biometric feature. The pixels generated by the circle are compared with the threshold and the intensity value with two conditions defined as follows.

Condition 1: Threshold value is added with the candidate value when the pixel presented in the circle brighter than the intensity value.
Condition 2: Threshold value is minus with the candidate value when the pixel presented in the circle darker than the intensity value.

Key points are identified based on these conditions; then, the orientation of the key points is assigned by computing the orientation and magnitude estimation process. The magnitude and direction of the key points are estimated using eqn (9 and 10)

$$m(x,y) = \sqrt{\big(L(x+1,y) - L(x-1,y)\big)^2 + \big(L(x,y+1) - L(x,y-1)\big)^2} \quad (9)$$

$$\theta(x,y) = atan2\big(L(x,y+1) - L(x,y-1)\big), \big(L(x+1,y) - L(x-1,y)\big) \quad (10)$$

In eqn (9)

(x,y) *is represnted as the magnitude of the key image*

In eqn (10),

$\theta(x,y)$ *is denoted as the orientation the key point image*

From the estimated value of m $m(x,y)$ and, $\theta(x,y)$ the image gradient values are estimated to assign the key point orientation. With the help of the gradient value, the histogram of the images is calculated by the degree of the histogram with 36 pins. Defined key point orientation, key descriptions are extracted by making candidate ear images 4 * 4 histogram orientation. The created images have 16 * 16 key points; each key point has 4 * 4 subdivisions sub-regions with 120 elements along with eight bins. The resulting key descriptor elements are normalized by the default threshold value of 0.2. The extracted element is equal to an entry value, which is considered to be the ear features, which are stored as a template.

Once the user attempts to access PHR data, initial authentication is performed in accordance with contextual authentication and biometric verification. The template matching process performs biometric verification; the ear features included by the user are matched with the template feature. The matching process is done according to the Hausdorff distance measure defined in Eqn (11).

$$d_H(X,Y) = \max\{\sup_{x\in X} \inf_{y\in Y} d(x,y), \sup_{y\in Y} \inf_{x\in X} d(x,y)\} \quad (11)$$

Sup – supremum, inf-infimum

In Eqn (11), $d_H(X,Y)$ Similarity between the user enter features with the template biometric features. The calculated similarity value is associated with the default threshold value of 0.2. Estimated values are the minimum for the threshold value. They are restricted from accessing PHR data; otherwise, users can access PHR data by providing the appropriate secret key. Once the user accepts the key, the specific PHR data is encrypted and the details are retrieved. The encryption process is performed using eqn (12).

$$M = Dec_{DK}(CT) \quad (12)$$

Therefore, the introduced elliptic curve cryptography (ECC) and biometric integrated multi-factor authentication process, effectively ensure user authentication, authentication, security, privacy and integrity. System performance is evaluated using experimental results and discussion, which is described in the following section.

IV. RESULTS AND DISCUSSION

This section describes the excellence of the Elliptic Curve Cryptography (ECC) and biometric integrated multi-factor authentication process based PHR data sharing and

access in the cloud environment. The execution process method uses two different datasets such as American Psychological Association (APA) (http://www.apa.org/research/responsible/data-links.aspx) and Mental Health Services Data Set (MHSDS) (http://content.digital.nhs.uk/mhsds). The dataset collects information from a variety of people, including young people, adults and children. These datasets contain different information on mental health issues, problems and disorders. Collected health information must be protected before being stored in a cloud environment. If the user fails to manage data security, unauthorized access or intermediate access will affect the quality of the data and alter the content. Changes in health information have implications for clinical analysis. Therefore, Elliptic Curve Cryptography (ECC) and biometric integrated multi-factor authentication process applied to ensure data security, privacy, authentication, authorization and integrity. The detailed work process is illustrated in Figure 1, and the respective discussions are analyzed in Section 3. The secure cloud data sharing and access process generated are evaluated using different security metrics. Encryption time, decryption time, execution time and user authentication accuracy. The system discussed and the encryption and decryption time results obtained using Python language version 3.6.5 are described in Table 1.

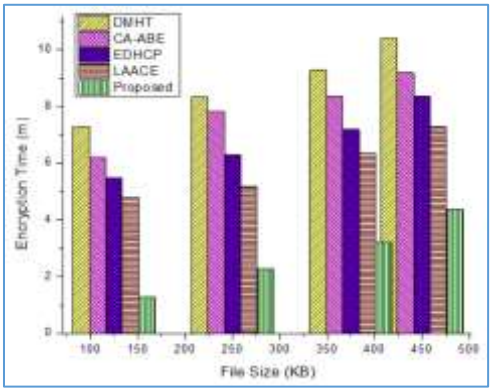
Table 1: (a) Encryption Time (m)

Method/ Data	DMHT	CA-ABE	EDHCP	LAACE	Proposed
125	7.289	6.19	5.47	4.8	1.27
250	8.319	7.83	6.28	5.17	2.28
375	9.279	8.35	7.18	6.34	3.19
450	10.39	9.19	8.36	7.27	4.36

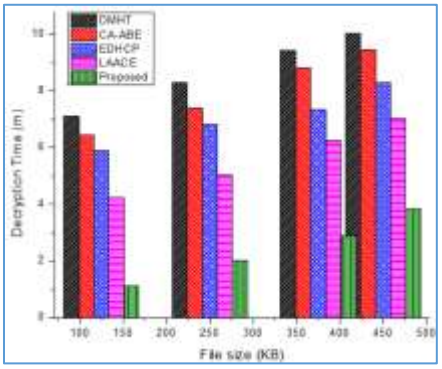
Table 1: (b) Decryption Time (m)

Method/ Data	DMHT	CA-ABE	EDHCP	LAACE	Proposed
125	7.10	6.45	5.89	4.23	1.12
250	8.28	7.39	6.83	5.02	2.03
375	9.42	8.82	7.35	6.25	2.89
450	10.02	9.45	8.29	7.02	3.85

Tables 1 (a) and (b) illustrated the encryption and decryption time of the introduced Elliptic Curve Cryptography (ECC) and biometric integrated multi-factor authentication process. The results obtained are compared with many other existing research works such as dynamic Merkle hash B+ tree algorithm (DMHT) Ramesh et al (2017) the ciphertext policy-attribute based encryption (CP-ABE) Doshi N et al (2019) elliptic curve Diffie-Hellman Crypto process (EDHCP) Subramanian et al (2020) and Lightweight Attribute with Access Control Encryption Techniques (LAACE) Prabhu kavin et al(2020). The effective generation of key encrypts the user information and shared data with minimum time. Not only this, the method also decrypts the data effectively. The respective graphical analysis is then shown in Fig 2 (a) and (b)



(a)



(b)

Fig 2: (a) Encryption time and (b) Decryption time of secure PHR data sharing and access process

Figure 2 illustrates the encryption and decryption time for accessing different secure PHR data sharing and cloud environment systems. From the analysis, the introduced Elliptic Curve Cryptography (ECC) and biometric integrated multi-factor authentication process method achieve a minimum time for encryption (2.775 m) and decryption (2.47 m) at different file sizes of the data sharing. The introduced method encrypts data with minimal time due to the effective key generation, sharing and secret key generation process. The encryption and decryption time obtained is very short compared to other security algorithms. Not only this, the Introduced method should consume minimum execution consume minimum execution time for data sharing, User authentication and data access process. The obtained execution time is illustrated in table 2 and fig 3

Table 2: Execution Time (m)

Method/ Data	DMHT	CA-ABE	EDHCP	LAACE	Proposed
125	6.89	5.38	4.89	4.28	1.23
250	7.29	6.89	5.038	4.49	1.89
375	8.478	7.12	6.32	5.13	2.03
450	9.189	8.027	7.39	6.48	2.79

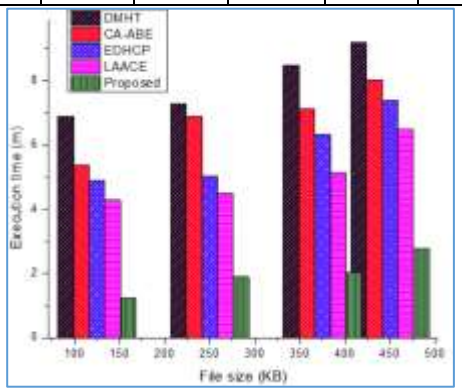


Fig 3: Execution time of secure PHR data sharing and access process

Figure 3 illustrates the execution time of different secure PHR data sharing and accessing in cloud environment systems. From the analysis, the introduced Elliptic Curve Cryptography (ECC) and biometric integrated multi-factor authentication process method attain minimum time for execution (1.98 m) at different file sizes. The introduced method achieves the minimum execution time due to the effective working process elliptic key pair generation and ear authentication process. The obtained execution time is low when compared to other methods such as dynamic Merkle hash B+ tree algorithm (DMHT) Ramesh et al (2017) the ciphertext policy-attribute based encryption (CP-ABE) Doshi N et al (2019) elliptic curve Diffie-Hellman Crypto process (EDHCP) Subramanian et al (2020) and lightweight attribute with access control encryption techniques (LAACE) Meddah N (2017) et al. As discussed in section 3, the ear biometric feature authenticates the user identity precisely. Then the system obtained authentication accuracy is illustrated in table 3.

Table 3: Authentication Accuracy (%)

Method/ Data	DMHT	CA-ABE	EDHCP	LAACE	Proposed
125	94.79	95.29	96.28	97.38	97.89
250	95.38	96.20	96.83	97.48	98.28
375	95.239	96.82	97.29	97.29	98.97
450	95.20	96.48	97.46	97.84	98.48

Table 3 illustrated that the authentication accuracy of introduced Elliptic Curve Cryptography (ECC) and biometric integrated multi-factor authentication process. The obtained results are compared with the several existing types of research works such as dynamic Merkle hash B+ tree algorithm (DMHT). Then the system obtained authentication accuracy is illustrated. Ramesh et al., (2017) the ciphertext policy-attribute based encryption (CP-ABE) Doshi N et al (2019) elliptic curve Diffie-Hellman Crypto process (EDHCP) Subramanian et al (2020) and lightweight attribute with access control encryption techniques (LAACE) Meddah N et al (2017). Then the relevant graphical analysis is shown in fig 4.

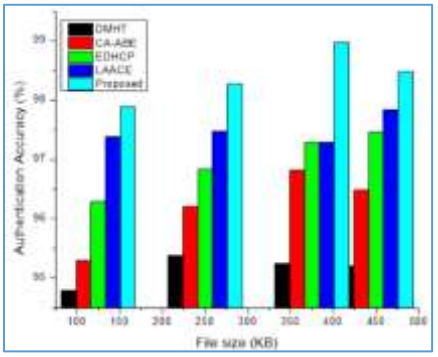


Fig 4: Authentication Accuracy

From the table 3 and Figure 4 that the introduced Elliptic Curve Cryptography (ECC) and biometric integrated multi-factor authentication process provides maximum accuracy (98.40%) of security to the shared health records compared to other methods such as Dynamic Merkle Hash B+ Tree algorithm (DMHT) (95.15%) Ramesh et al., (2017) the ciphertext policy-attribute based encryption (CP-ABE) (96.19%) Doshi N et al (2019) Elliptic Curve Diffie-Hellman Crypto process (EDHCP) (96.92%) Subramanian et al (2020) And Lightweight Attribute with Access Control Encryption Techniques (LAACE) (97.45%) Meddah N et al (2017). Therefore, the Elliptic Curve Cryptography (ECC) and biometric integrated multi-factor authentication process maintain data security, privacy, and confidentiality with less computation time, overheads, and accuracy than other methods.

V. CONCLUSION

Thus, the paper examines Elliptic Curve Cryptography (ECC) and biometric integrated multi-factor authentication process to provide data security for shared personal health records. Initially, PHRs will be stored in encrypted form on a third-party server. The encryption is done according to the elliptic pair of key generation. The generated keys are shared between the owner and the server. This helps the user to authenticate because user lists are maintained by the server, minimizing data transfers and unauthorized access. Each time, the user authenticated via the contextual recognition process and ear biometric features match with the template to verify the authorized users. Once the user

authenticated by the developed system, the PHR data access permission is established with the respective key value. The system discussed ensures data security, confidentiality and integrity with 98.40% accuracy and minimum execution time. In future, optimization algorithms and deep learning techniques are incorporated to maintain the data security.

REFERENCES

[1] Pancholi, Vishal R., and Bhadresh P. Patel. "Enhancement of cloud computing security with secure data storage using AES." International Journal for Innovative Research in Science and Technology 2, no. 9 (2016): 18-21.

[2] Dang, L. Minh, Md Piran, Dongil Han, Kyungbok Min, and Hyeonjoon Moon. "A survey on internet of things and cloud computing for healthcare." Electronics 8, no. 7 (2019): 768.

[3] Li, Jin, Yinghui Zhang, Xiaofeng Chen, and Yang Xiang. "Secure attribute-based data sharing for resource-limited users in cloud computing." Computers & Security 72 (2018): 1-12.

[4] Sookhak, Mehdi, F. Richard Yu, and Helen Tang. "Secure data sharing for vehicular ad-hoc networks using cloud computing." In Ad Hoc Networks, pp. 306-315. Springer, Cham, 2017.

[5] Li, Ruixuan, Chenglin Shen, Heng He, Xiwu Gu, Zhiyong Xu, and Cheng-Zhong Xu. "A lightweight secure data sharing scheme for mobile cloud computing." IEEE Transactions on Cloud Computing 6, no. 2 (2017): 344-357.

[6] Li, Jin, Yinghui Zhang, Xiaofeng Chen, and Yang Xiang. "Secure attribute-based data sharing for resource-limited users in cloud computing." Computers & Security 72 (2018): 1-12.

[7] Rao, Y. Sreenivasa. "A secure and efficient ciphertext-policy attribute-based signcryption for personal health records sharing in cloud computing." Future Generation Computer Systems 67 (2017): 133-151.

[8] Zhang, Leyou, Qing Wu, Yi Mu, and Jingxia Zhang. "Privacy-preserving and secure sharing of PHR in the cloud." Journal of medical systems 40, no. 12 (2016): 267.

[9] Thwin, Thein Than, and Sangsuree Vasupongayya. "Blockchain based secret-data sharing model for personal health record system." In 2018 5th International Conference on Advanced Informatics: Concept Theory and Applications (ICAICTA), pp. 196-201. IEEE, 2018.

[10] Kumar, Rakesh, and Rinkaj Goyal. "Modeling continuous security: A conceptual model for automated DevSecOps using open-source software over cloud (ADOC)." Computers & Security 97 (2020): 101967.

[11] Song, Young G., Richard Sah, Moo Chan Song, and Frank C. Pesek. "Efficient data transfer for cloud storage by centralized management of access tokens." U.S. Patent 9,294,550, issued March 22, 2016.

[12] Maes, Stephane H., Rajeev Bharadhwaj, Travis S. Tripp, Kevin Lee Wilson, Petr Fiedler, and John M. Green. "Cloud application deployment." U.S. Patent 9,923,952, issued March 20, 2018.

[13] Xiong, Hu, Hao Zhang, and Jianfei Sun. "Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing." IEEE Systems Journal 13, no. 3 (2018): 2739-2750.

[14] Zhang, Leyou, Qing Wu, Yi Mu, and Jingxia Zhang. "Privacy-preserving and secure sharing of PHR in the cloud." Journal of medical systems 40, no. 12 (2016): 267.

[15] Liu, Jianghua, Xinyi Huang, and Joseph K. Liu. "Secure sharing of personal health records in cloud computing: ciphertext-policy attribute-based signcryption." Future Generation Computer Systems 52 (2015): 67-76.

[16] Shabir, Muhammad Yasir, Asif Iqbal, Zahid Mahmood, and AtaUllah Ghafoor. "Analysis of classical encryption techniques in cloud computing." Tsinghua Science and Technology 21, no. 1 (2016): 102-113.

[17] Dhote, C. A. "Homomorphic encryption for security of cloud data." Procedia Computer Science 79 (2016): 175-181.

[18] Kakkad, Vishruti, Meshwa Patel, and Manan Shah. "Biometric authentication and image encryption for image security in cloud framework." Multiscale and Multidisciplinary Modeling, Experiments and Design 2, no. 4 (2019): 233-248.

[19] Joseph, Teena, S. A. Kalaiselvan, S. U. Aswathy, R. Radhakrishnan, and A. R. Shamna. "A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment." Journal of Ambient Intelligence and Humanized Computing (2020): 1-9.

[20] Rehman, Faisal, Sana Akram, and Munam Ali Shah. "The framework for efficient passphrase-based multifactor authentication in cloud computing." In 2016 22nd International Conference on Automation and Computing (ICAC), pp. 37-41. IEEE, 2016.

[21] Ramesh, D., Mishra, R. & Edla, D.R. Secure Data Storage in Cloud: An e-Stream Cipher-Based Secure and Dynamic Updation Policy. Arab J Sci Eng 42, 873–883 (2017). https://doi.org/10.1007/s13369-016-2357-2

[22] Masala G.L., Ruiu P., Grosso E. (2018) Biometric Authentication and Data Security in Cloud Computing. In: Daimi K. (eds) Computer and Network Security Essentials. Springer, Cham. https://doi.org/10.1007/978-3-319-58424-9_19

[23] Suresh, D., Florence, M.L. Securing Personal Health Record System in Cloud Using User Usage Based Encryption. J Med Syst 43, 171 (2019). https://doi.org/10.1007/s10916-019-1301-x