Original Article

Improved CP-ABE Based Crypto Technique To Secure Ehrs With Access Policy-Based Authentication Schemes

S.Prathima[1], Dr.C.Priya[2]

[1]Research Scholar Department of Computer Science Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India prathismanian@gmail.com

[2]Associate Professor & Research Supervisor Department of Information Technology, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India drcpriya.research@gmail.com

DOI: 10.47750/pnr.2022.13.S09.281

Abstract

Every medical service center handles the health records in the conventional Electronic Health Record (EHR) management system. Therefore, in Cloud Computing (CC), EHR is stored; however, that can be susceptible to numerous attacks as the sensitive data is transmitted over a public channel. Many attempts have been made by prevailing research techniques to ameliorate the EHR's Security Level (SL); however, the security problem continues to exist. This work has put forward an Improved Ciphertext-Policy centered Attribute-Based-Encryption (ICP-ABE) to secure EHR with an access policy-centered authentication scheme for solving this issue. EHR data collections, secure uploading, and secure downloading are the '3' phases that are entailed in the proposed method. At first, the input EHR data is amassed; after that, the data is safely uploaded to the Cloud Server (CS). Attribute extraction, significant attribute selection by LF-LOA, access policy creation by selected attributes, and securely uploading the input file into the CS by wielding the ICP-ABE algorithm are the '4' phases that are encompassed in this uploading process. Verifying access policy, permission to key access, and downloading and decrypting the data are the '3' sub-phases involved in the last phase, which is the secure downloading phase. The proposed technique-centered secure EHR data storing is analogized to the prevailing techniques in an experimental assessment. When weighed against the existent research methodologies, the proposed technique achieves superior performance.

Keywords: Levy Flight based Lion Optimization Algorithm (LF-LOA), Improved CiphertextPolicy based Attribute-Based Encryption (ICP-ABE), Access policy creation, Electronic Healthcare Record (EHR), and a secret key.

I. INTRODUCTION

Applying CC technologies in eHealth systems has evinced immense potential and a lengthy list of unprecedented benefits in governing the EHRs in the real world because modern eHealth systems are data-intensive [1]. CC is a current concept in digital technology, which is widely wielded in the healthcare industry [2]. From conventional information technologies to integrated services provided by cloud providers, the notion of sharing, processing, along with storing the data has been changed by CC [3]. In the cloud, EHRs are wanted to be stored in encrypted form with the growth of CC along with the demands for the patient's data privacy [4]. These days, structured medical data are kept in standard digital formats say, EHR or Personal Health Records (PHR). For maintaining medical connectivity globally, E-Health systems are a better choice and may access the clinical information on a prerequisite basis [5]. EHR includes sensitive and confidential data about the patient (for instance: diagnoses, patients' tests, treatment accompanied by information on the patients' medical history) [6]. The record constitutes the patient's vitals, physical signs: weight, height, symptoms, along with signs. These data are named to be straightforward data points yet are intricate to manage [7]. Even though EHR contains confidential information for patient diagnosis along with treatment, it is required to be often shared amongst diverse partakers like healthcare providers, insurance

firms, pharmacies, along with medical researchers [8]. It can be accessed by particular hospitals with the patient's permission in order that medical personnel can simply probe for pertinent information about the patient [9]. But, the chance of attacks on patient records along with information privacy has been increased by keeping electronic copies of the patient health as well as history [10]. By providing every patient with a username and password, these E-health records can be protected to prohibit unauthorized access. Securing the data stored by encrypting it in the cloud is the subsequent step with a special key that can be only be acknowledged by the data owner [11]. The most generally utilized mechanism to guarantee user's confidentiality in the cloud environment is encryption [12].

The major basic protection method used by each model is encryption and data transmitted to the cloud is in the encrypted form [13]. Prior to transmission from sender to receiver, data should be converted into ciphertext utilizing encoding methodologies in encryption methods. By employing the decoding technique, the original message can be perceived by the receiver following the reception of data [14]. ABE is exploited to contribute Fined-Grained Access Control (FGAC) of the EHR data. ABE still experiences a severe issue that the access policy may seep out EHR owner's privacy, even though ABE systems could offer protected Access Control (AC) for the EHR data in an EHR scheme [15]. Since in an ABE system, to give FGAC in cloud storage the identity of every user is delineated [16]. This point-to-point encryption server utilizes numerous cases; however, this is not adequate to fulfil the demands and creates a disturbance in AC [17]. The AC model is a manner in which assurance is given that the documents are safely saved in cloud storage with suitable access protection. For secure exchange of EHR, it scrutinizes, examines, along with configures healthcare cloud as well as services [18]. While offering health services, AC is vital for protecting patient privacy. AC refers to only transmitting patient documents to authorized doctors [19]. But, the majority of the current AC systems for health services are rigid. To execute efficient privacy-preserving, the proposed methodology utilizes an access policy-centered modified Ciphertext Policy Attribute-Based-Encryption (CP-ABE) algorithm.

The rest of the paper is arranged as: The methodologies associated with diverse encryption methods to secure EHR are explicated in Section 2. Section 3 expounds on the proposed attribute-centered access technique for secure sharing of EHR data. Section 4 examines the proposed system's performance. Section 5 concludes the paper.

II. LITERATURE SURVEY

Seyed Morteza Pournaghi *et al.* [20] exhibited a method centered on blockchain technology to offer permission to enter into a data source along with permit the transfer of these types of rights amongst users. Utilizing attribute-centered encryption, the MedSBA system tries to protect patient privacy together with regulate the fine-grain access to medical data. To FGAC of patients on their medical records, the technique had utilized '2' attribute-centered kinds: Key Policy (KP-ABE) along with CP-ABE. Generating medical content, storing, along with utilizing PHI information were the '3' phases in the MedSBA scheme. For distributing the access level on the network, the methodology utilized a private and public blockchain, thus an entity couldn't infringe on security features alone. The technique had the disadvantage that the entire members of the network require to save a copy of the blockchain information.

Xueyan Liu *et al.* [21] displayed an unidentified EHRs sharing methodology centered on decentralized hierarchical ABE. The technique had '3' steps (1) To accomplish FGAC and scalable data AC along with evade a blockage, multiple Attribute Authority (AA) ABE was leveraged. For encrypting numerous files in one operation, a hierarchical access tree was wielded, thus saving calculation and storage load very much. (2) To oppose the collusion attack of users, a user's Global Identifier (GID) was established. Next, for preventing numerous AAs as of constructing a complete profile utilizing the user's GID, an anonymous key generation mechanism was furnished. (3) Double verification centered on the verification tag along with convergent key was done to guarantee the accuracy and integrity of EHRs. The methodology was unsuccessful to solve the user revocation issue that is if any alterations happen in the user's attribute or any changes that occur in the user's roles, it requires updating each attribute which is needed to create the security system.

Sana Belguith *et al.* [22] explicated a responsible privacy-preserving attribute-centered methodology, known as InsPAbAC that merges ABE and attribute-centered signature methods to safely share outsourced data contents through the public CSs. The system initialization procedure SYS_INIT was carried out during the 1st phase. If the data owner desires to disclose data files with another

cloud user, the 2nd phase happens, centered on the data storage procedure STORE along with the data retrieval procedure BACKUP. The 3rd phase happens when there was a requirement for users' anonymity revocation, depending on the implementation of the inspection procedure INSPEC, whilst the 1st and 2nd phases were obligatory for outsourcing data files to the CSs. The system performance was affected by too much computation cost on the data user side.

Gandikota Ramu *et al.* [23] exhibited a modified CP-ABE system with user revocation to reinforce the data outsourcing scheme in cloud architecture. The key-escrow and revocation difficulties are handled by the system. 1) By utilizing '2'-authority computation betwixt the key generator authority along with CS, the key-escrow issue was solved. 2) To attain fine-grained user revocation, an immediate attribute modification methodology was utilized. By curbing the system managers along with others as of accessing the data that didn't have sufficient credentials, the system enriched EHR privacy along with confidentiality in CSs. Since the need for security parameters was a huge size that consumes more time to encrypt the data, the technique had lost the higher efficacy.

Hao Wang *et al.* [24] established a cryptographic primitive termed Combined Attribute-Based or Identity-Based Encryption and Signature (C-AB/IB-ES) to accomplish diverse roles of ABE, IBE, together with IBS in the'1' cryptosystem. This really ease the system's management, along with didn't require initiating diverse cryptographic systems for diverse security needs. Moreover, to make sure the integrity along with traceability of medical records, the technique utilized blockchain methodologies. To ensure FGAC for encrypted data, the system utilized ABE along with Identity-Based Encryption (IBE) for encrypting data. Identity-Based Signature (IBS) was employed to execute digital signatures. Owing to the scalability problem in the blockchain method the security was decreased.

Yi Liu *et al.* [25] explicated an FGAC EHR system that was confirmed secure in the benchmark model in the decisional parallel bilinear Diffie-Hellman (DH) exponent assumption appropriate for mobile CC. The calculation needed for the EHR's encryption was divided into an offline as well as an online phase in the EHR AC system. Also, when EHR data along with access policies turn out to be recognized, the online phase quickly assembles the final ciphertexts. The EHR AC scheme permits access policies encoded in linear secret sharing systems. Yielding offline ciphertext prior to knowing the EHR data engenders augmented computational time since there might be a possibility of occurring mismatch betwixt the assumed along with original EHR data.

III.THE ACCESS POLICY BASED AUTHENTICATION OF SECURE STORAGE

There has been an increasing trend to wield the cloud for larger-scale data storage with the quick expansion happening in cloud services. Several healthcare organizations have initiated moving EHR to cloud-centered storage systems owing to the rising fame of cloud storage. But, this has elevated the significant security problem of how to preserve and stop unauthorized access to EHR data stored in a public cloud. To safeguard the data's security stored in the cloud, numerous cryptographic AC schemes have been proposed by incorporating cryptographic methodologies with AC models; however, these methods are incompetent to tackle the issue of the storage in CC.

This work proposed an improved CP-ABE-centered encryption method to secure EHR with an access policy-centered authentication scheme to conquer these issues. EHR data collection, secure upload, and secure download are the '3' steps in the proposed method. Initially, the EHR data is amassed; then, the data are safely uploaded to the CS. This uploading phase encompasses '4' sub-phases that are, attribute extraction, attribute selection, access policy creation, and securing the EHR data. The input file's attributes are extracted; then, the significant attributes are chosen by utilizing Levy Flight-centered Lion Optimization Algorithm (LF-LOA). Next, the access policy is developed; then, the data is securely stored in the CS utilizing the Improved Ciphertext-Policy Attribute-Based Encryption (ICP-ABE) algorithm with the assistance of the created access policy. Securely, the user can download their EHR from a CS after uploading the data. Verifying access policy, permission to key access, and downloading and decrypting the data are the '3' steps entailed in the downloading phase. Figure 1 portrays the block diagram of the proposed research method

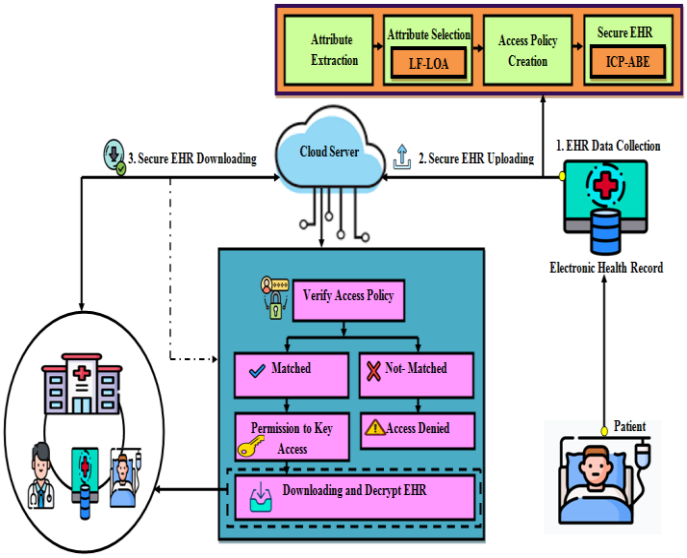

Figure 1: Schematic representation of the proposed system

A. EHR data

The systematized compilation of patient data and information about the population is called an EHR, which is stored in a digital format. EHR may encompass a variety of information, entailing medical history, demographics, medication together with allergies, laboratory test outcomes, immunization status, radiology images, vital signs, and individual details such as age, weight, along with billing details. Document (.Doc), Image (.jpeg, .png), Excel format (.xlsx) etc are the diverse kind of file formats that are entailed. The amassed data is expounded as follows,

$$Z_s = \{z_1, z_2, z_3, ..., z_n\}, \quad (or) \;\; z_i, i = 1,2,3,....,n \tag{1}$$

Where, the collected dataset is denoted by Z_s , the data in EHR is indicated as z_i , and the n-number of data proffered in the EHR record is represented by z_n

B. Secure Upload

Next, the data is securely uploaded to the CS. The original data is converted into the cryptographic format in this phase. Therefore, attribute extraction, attribute selection, access policy creation, along with securing the data are the '4' stages of the uploading phase. Every stage is explicated in the sub-section as follows: -

1) Attribute extraction

The input file's attributes are extracted as of the input EHR. Therefore, file type, file location, file size, file size on disk, created date, etc are the attributes. Equation (2) articulates the input EHR data's attributes as,

$$\vec{a}(Z_s) = \vec{a}(z_1), \vec{a}(z_2), ..., \vec{a}(z_n), \; (or) \; \vec{a}(z_i) \tag{2}$$

Where, the attributes of the input record are delineated as $\vec{a}$.

2) Attribute selection using LF-LOA

By employing the LF-LOA algorithm, the vital attributes as of the extracted attributes are selected. An initial population is constructed by a group of arbitrarily yielded solutions termed Lions in LOA. In the initial population ($\%N$) a few of the lions are chosen as nomad lions along with the remaining population (resident lions) is arbitrarily bifurcated into R subsets termed prides. M Percent of the pride's members are regarded as female along with remaining is regarded as male, whilst this rate (sex rate $(\%M)$) in nomad lions is contrariwise. The finest acquired solution in past iterations is known as the best-visited position for every lion along with amid the optimization process is updated gradually. The random value differs from 0 to 1 in normal LOA. This variation may fall into the local optimum solution, which will degrade the attribute selection's performance. Rather than fixing the random value, this research technique entails the levy flight that selects the better attributes to solve this issue. In the solution space, the LOA firstly produced the population randomly. It considered every individual solution as a "lion (i.e, considered as attributes)". For a N_v dimensional optimization issue, a lion is delineated as,

$$\delta = \left\{c_1, c_2, c_3, ..., c_{N_v}\right\} \tag{3}$$

Where, the initialized population set is described as δ and the N_v population is delineated as c_{N_v} . Then, by examining the cost function, the cost (fitness value of every lion) is found by,

$$f(\delta) = f\left\{c_1, c_2, c_3, ..., c_{N_v}\right\} \tag{4}$$

To discover the prey for food, the entire pride lions in the resident territory set out for hunting in a group. Here, centered on a fitness function, the hunters are split into 3 subgroups. The group with the maximum cumulative members' finesses is regarded as Center, along with another '2' groups contemplate as '2' wings. In the next equation, a dummy prey is regarded in the hunter's center:

$$D_p = \frac{\sum_{i=1}^{n} \beta_i \left(c_1, c_2, c_3, ..., c_{N_v}\right)}{\vec{N}(\beta_i)} \tag{5}$$

Where, the dummy prey is symbolized by D_p , the hunters are depicted by β_i along with the total number of hunters is signified by $\vec{N}(\beta_i)$. If the hunter enhances its fitness, the prey will run away as of the hunter during the process of hunting and discover a novel position utilizing the next equation:

$$D_p^{'} = D_p + \psi \times o_i \times \left(D_p - H(\beta_i)\right) \tag{6}$$

Where, the current position is $D_p^{'}$, the hunter's new position who attacks the prey is $H(\beta_i)$, the percentage of enhancement in the hunter's fitness value is o_i , and the random steps which are drawn from a Levy distribution for larger steps are denoted by ψ :

$$\psi = Levy \sim e^{-\omega}, (1 < \omega \leq 3) \tag{7}$$

Where, the current generation is symbolized by e and the step length is delineated by ω . The new position of hunter which are belonging both the left together with right wing is produced as,

$$H(\beta_i)' = \begin{cases} k_d\left(\left(2*D_p - H(\beta_i)\right), D_p\right), & \left(2*D_p - H(\beta_i)\right) < D_p, \\ k_d\left(D_p, \left(2*D_p - H(\beta_i)\right)\right), & \left(2*D_p - H(\beta_i)\right) > D_p. \end{cases}$$

Then, the hunter's new position at the prey (8) position in center wing is scrutinized as follows,

$$H(\beta_i)' = \begin{cases} k_d\left(H(\beta_i), D_p\right), & H(\beta_i) < D_p \\ k_d\left(D_p, H(\beta_i)\right), & H(\beta_i) > D_p \end{cases} \quad (9)$$

Nomad lions roam in an adaptive roaming methodology utilizing equation (11):

$$No(\beta_{ij}) = \begin{cases} \beta_{ij} & if \ \ (k_d)_j > \vec{p}_{ro} \\ (k_d)_j & otherwise \end{cases} \quad (10)$$

Where, the present position of i^{th} nomad lion is $No(\beta_{ij})$, the dimension is j, a uniform Random Number (RN) within [0, 1] is $(k_d)_j$, the randomly produced vector in search space is k_d along with a likelihood that is computed for every nomad lion independently is $\vec{p}_{ro}$. As exhibited in the equation, the mating process is done betwixt '2' diverse lions to generate '2' offspring because prides and nomads are considered unisex.

$$\varepsilon_j^1 = \psi * \beta_j^i + \sum \frac{1-\psi}{\sum_{i=1}^{N_r} Y_i} * \beta_j^u * Y_i \quad (11)$$

$$\varepsilon_j^2 = (1-\psi) * \beta_j^i + \sum \frac{\psi}{\sum_{i=1}^{N_r} Y_i} * \beta_j^u * Y_i \quad (12)$$

Where, the dimension is j, the '2' new offsprings is defined by ε_j^1 and ε_j^2, Y_i equivalent 1 if Lions i and u are chosen for mating, or else it equivalents 0, and N_r is the number of residents in a pride

Input: Extracted attributes, $\vec{a}(z_i)$

Output: important attributes

Begin

Initialize population δ , pride and nomad lions, and maximum iteration ξ .

Set iteration $\tau = 1$

While $(\tau \le \xi)$ **do**

Divide hunter group into left, centre, and right-wing positions

Find the new position of the hunter using,

$$D_p^{'} = D_p + \psi \times o_i \times \left(D_p - H(\beta_i)\right)$$

if $(D_p == left \,\&\, \&right)$ {

Update the position of the hunter using,

$$H(\beta_i)^{'} = \begin{cases} k_d\left(\left(2 * D_p - H(\beta_i)\right), D_p\right), & \left(2 * D_p - H(\beta_i)\right) < D_p, \\ k_d\left(D_p, \left(2 * D_p - H(\beta_i)\right)\right), & \left(2 * D_p - H(\beta_i)\right) > D_p. \end{cases}$$

} **else** {

Update the position of the hunter using,

$$H(\beta_i)^{'} = \begin{cases} k_d\left(H(\beta_i), D_p\right), & H(\beta_i) < D_p \\ k_d\left(D_p, H(\beta_i)\right), & H(\beta_i) > D_p \end{cases}$$

} **end if**

Produce new cubs in nomad lions

Calculate fitness

Set $\tau = \tau + 1$

Return important attributes

End while

End

Fig.2. pseudo-code for LF-LOA

The proposed LF-LOA's pseudo-code is displayed in figure 2. Therefore, the hunter position updation process is explained by the pseudo-code. Left, center, and right-wing positions are the '3' hunter groups. The fitness value is computed subsequent to the position updation; if the fitness level is not met, then the iteration step is augmented. Until the fitness function is reached, the process is repeated. Lastly, significant attributes are acquired.

C. Access Policy Creation

The access policy is developed by utilizing the chosen attributes following the attribution selection. The selected attribute's combination is called the access policy. For the uploaded file, this Access Policy will be constructed, and a copy will be provided to the uploaded user for future authentication. Access policy creation is obtained as:

$$F = \sum_{i=1}^{n} \vec{a}(z_i) \tag{13}$$

Where, the created access policy is explicated as F .

D. Secure data transfer using ICP-ABE algorithm

By utilizing the ICP-ABE algorithm, the file is encrypted along with is safely uploaded to the server. A data sender encrypts the message utilizing a conventional encryption scheme in CP-ABE Scheme. An access policy is symbolized in form of access structure over attributes in the ciphertext. The user that is competent in accessing the cipher-text is specified by the access structure. On the basis of a polynomial equation and random values, the access structure is formed in a regular CP-ABE algorithm; this process is not a secure process. Hence, this study method wielded the Hessian Node Selection process rather than the polynomial-based access structure. If only the attributes match the access policy related to the encrypted data, the users decrypt the ciphertext. However, security problems prevail in the CP-ABE algorithm. Hence, this study method considered the access as the Secret Key (SK) along with it will be added in the file Encryption Time (ET) as well as it will be subtracted in the Decryption Time (DT). In the CP-ABE algorithm, this type of improvement is carried out. Server initialization, private key generation, encrypting the plaintext, and decrypting the ciphertext are the '4' steps involved in the algorithm.

1)Server initialization:

The implicit security parameter is taken as the setup algorithm as well as the public parameters (L_k) together with a master key (Q_k) are given as output. It selects a bilinear group Gr_0 of prime order q with generator w . Then, it will opt '2' random exponents $\alpha, \beta \in Z_p$. The public key is given as:

$$L_k = \left(Gr_0, w, h = w^{\upsilon}, \quad f = w^{1/\upsilon}, e(w,w)^{\eta}\right) \tag{14}$$

The master key is:

$$Q_k = \left(\upsilon, w^{\eta}\right) \tag{15}$$

2)Private-Key generation:

A set of attributes is offered by the user, and a user SK(F) is generated by the server. The generation rule is $F = GenerateUserKey\left(Q_k, \vec{a}(z_i)\right)$. The server opts for the

RN $x, \left(x \in Z_p\right)$, after that, for every attribute $j \in \vec{a}\left(z_i\right)$, chooses an RN $x_j \in Z_p$, computes the attribute SKs B_j and $B_j^{'}$. Finally, it merges all attribute private keys to form the user SK F along with returns F to user. The SK is of the form

$$F = \left\{ B = w^{\frac{\eta+\upsilon}{\upsilon}}, \forall j \in \vec{a}\left(z_i\right): B_j = w^{x}.H\left(j\right)^{x_j}, B_j^{'} = w^{x_j} \right\} \tag{16}$$

3)Data encryption:

The public key PK, the plaintext message z_i, and an AC policy $\left(CT, \gamma\right)$ are taken as input by the encryption algorithm; next, it selects random metrics $\vec{s}, \vec{v}_2, ..., \vec{v}_n \in Z_p$ thus the parameters are chosen on the basis of the hessian node selection and delineates the vector $\vec{v} = \left(\vec{s}, \vec{v}_2, ..., \vec{v}_n\right)$. The algorithm calculates the inner product $\lambda_i = CT_i.\vec{v}$ for each row CT_i of CT along with then it selects a random exponent $x_i \in Z_p$ along with outputs the ciphertext as follows:

$$CT = \left(\left(CT, \gamma\right), T = z_i.e\left(w, w\right)^{\upsilon\vec{s}}, T_0 = w^{\vec{s}}, \left\{T_{i,1} = w_1^{\lambda_i} h_{\gamma(i)}^{-x_i}, T_{i,2} = w^{x_i}\right\}_{i=1}^{l}\right) \tag{17}$$

D. Secure Download

To download the EHR, this is the safe authentication phase. From the CS, the user can download their EHR in a protected way. Verification of access policy, permission to key access, download, and decryption are the '3' sub-stages in the secure download stage.

E. Verification of Access Policy

The user requests $\left(ur\right)$ the file to be downloaded from the CS in this step. Next, the system asks for the corresponding Access Policy for the requested file to the user. The system deduces the requested user as the owner of the requested file if the requested user offers the accurate Access Policy. Or else, the download process is refused by the system. The verification process is articulated as follows

F. Permission to Key Access

The scheme lets the user to download the requested file as well as offers the decryption keys to decrypt the encrypted EHR file after the authentication process.

G. Download and Decryption

Lastly, utilizing this system, the requested user can safely download the uploaded file and can be competent to decrypt the file with the help of decryption keys. From the server, the user gets ciphertext together with decrypts ciphertext by utilizing its private key F to attain the plaintext data z_i. The decryption rule is,

$$z_i = Decrypt\left(CT, F\right) \tag{18}$$

The original input data is decrypted by utilizing equation (18). Therefore, for further process, the decrypted data is wielded

IV. RESULTS AND ANALYSIS

In the following section, the performance of the proposed model is analyzed. The proposed ICP-ABE-based encryption technique to secure EHR transfers that uses an access policy-based authentication scheme is developed in Java as the working platform.

A. Performance Evaluation

On the basis of ET, DT, and security, the performance investigation of the proposed ICP-ABE algorithm with prevailing DH, Rivest Shamir Adleman (RSA), Elliptic Curve Cryptography (ECC), and CP-ABE is conducted. After that, the upload time along with download time for the proposed ICP-ABE methodology are examined.

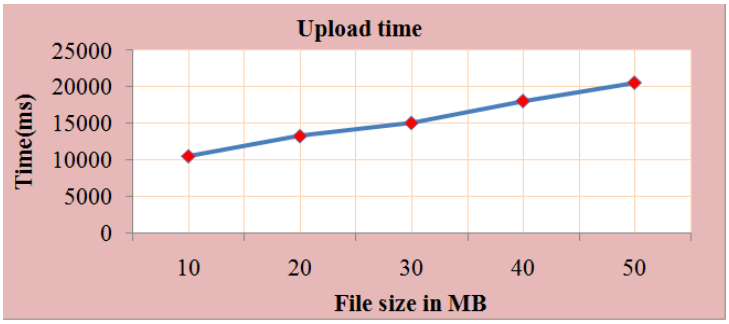

TABLE 1: PERFORMANCE EVALUATION OF THE EXISTING ALGORITHMS WITH THE PROPOSED ICP-ABE

(a) Encryption time

File size in MB	Diffie-Hellman	RSA	ECC	CPABE	Proposed ICP-ABE
10	1834	1375	1102	964	768
20	2614	2215	2208	1967	1357
30	3837	3314	3098	2874	2598
40	4912	4268	3821	3482	3047
50	5889	5431	5089	4912	4574

(b)Decryption time

File size in MB	Diffie-Hellman	RSA	ECC	CPABE	Proposed ICP-ABE
10	1812	1812	1812	1812	1812
20	2724	2724	2724	2724	2724
30	3894	3894	3894	3894	3894
40	4874	4874	4874	4874	4874
50	5974	5974	5974	5974	5974

(c) Security analysis

Methods	Security (%)
Diffie-Hellman	86.9321
RSA	88.2397
ECC	90.6845
CPABE	92.8345
Proposed ICP-ABE	95.6234

1)Analysis

Regarding ET, DT, and SLs, the performance of the ICP-ABE with the prevailing methodologies is investigated in Table 1. The time taken to convert the plain text into ciphertext is called the ET. The time taken for the conversion of ciphertext into plain text is termed the DT. In respect of files-size, the ET and DT are computed. The file size differs from 10MB to 50MB. The methodology DH takes more time for encryption and decryption than other RSA, ECC, and CP-ABE techniques, as exhibited in Table 1 (a) and (b), while the proposed ICP-ABE takes lesser time than the other techniques. For encryption and decryption, the CP-ABE methodology takes a medium time than the prevailing DH, RSA, and ECC approaches, which consume a larger time to encrypt and decrypt data; however, it consumes more time than the proposed ICP-ABE technique. On the basis of SL, table 1 (c) exhibits the performance. When analogized

to the DH and RSA methodologies, the proposed ICP-ABE, ECC, and CPABE have enhanced SLs. The aforementioned discussion expresses that the proposed ICP-ABE technique accomplished better performance than the prevailing methodologies.

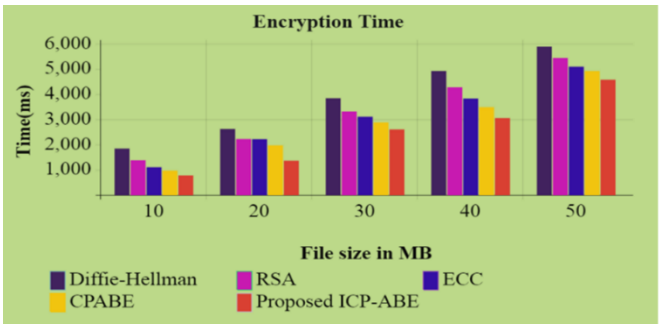

Fig 3. Uploading time for the proposed method

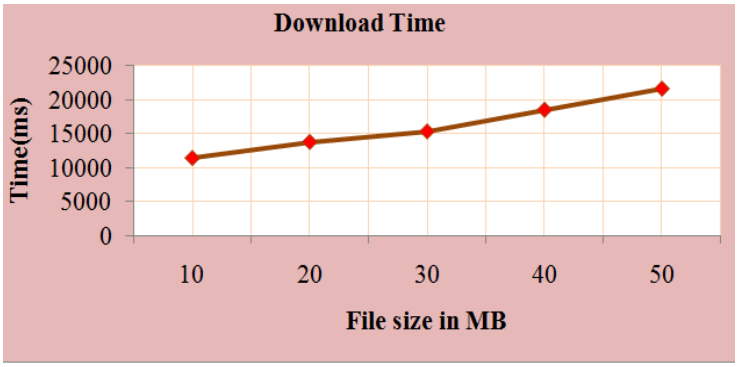

Fig 4. Downloading time for the proposed method

The upload time along with download time taken by the proposed methodology are displayed in figure 3,4. To upload the file of size 10MB, the proposed ICP-ABE algorithm takes 10457ms, whereas it takes 13214ms, 15024ms, 18047ms, and 20568ms for 20MB, 30MB, 40MB, and 50MB, respectively. Similarly, for the download time, the method takes 11347ms for the file size of 10MB, and for 20MB, 30MB, 40MB, and 50MB, it takes 13714ms, 15267ms, 18457ms, and 21578ms, respectively

B. Comparative Analysis

Centered on ET and DT, SL, and memory usage on encryption along with decryption, this part involves the comparative investigation of the proposed ICP-ABE algorithm with the prevailing DH, RSA, ECC, and CPABE algorithms. Next, regarding the attribute selection time and fitness vs iteration, the performance investigation of the proposed LF-LOA along with the prevailing Sandpiper Optimization Algorithm (SOA), Horse Optimization Algorithm (HOA), Rat Optimization Algorithm (ROA), and Lion Optimization Algorithm (LOA) is displayed.

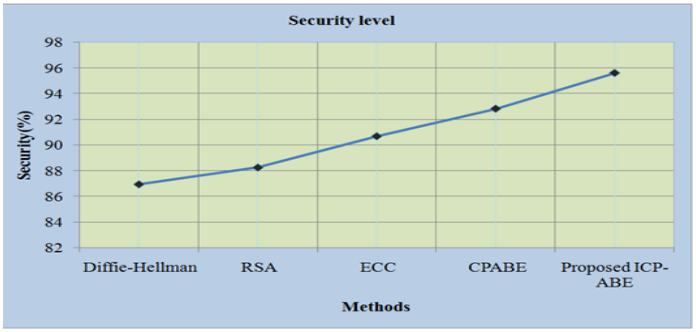

Fig.5. Encryption time for the proposed and existing methods

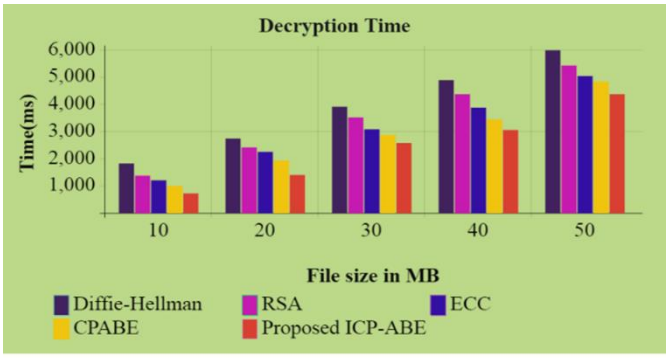

Fig.6. Decryption time for the proposed and existing methods

1). Analysis

The pictorial depiction of comparative investigation for the proposed ICP-ABE methodology with the existent methods with respect to ET and DT is evinced in figure 5,6. For encryption and decryption, the other techniques take 1834ms, 1375ms, 1102ms, and 764ms, respectively, and 1812ms, 1365ms, 1189ms, and 986ms, for the same size. For the same size, the other methods take 1834ms, 1375ms, 1102ms, and 764ms for encryption and 1812ms, 1365ms, 1189ms, and 986ms for decryption. For the rest of the file sizes, the proposed methodology has 1357ms, 2598ms, 3047ms, and 4574ms to encrypt the data, and the technique takes 1389ms, 2564ms, 3045ms, and 4357ms to decrypt the

data. The CPABE algorithm takes medium time for encryption and decryption whereas the DH, RSA, and ECC methods take longer time than the ICP-ABE method for all file sizes. For the rest of the file sizes, when analogized to the ICP-ABE technique, the prevailing techniques consume a long time to encrypt and decrypt the data.

Fig.7. Security level of the proposed and existing methods

1). Analysis

The pictorial depiction of security analysis for the proposed ICP-ABE and prevailing DH, RSA, ECC, and CPABE algorithms are illustrated in figure 7. In this, the security of 86.9321% has been achieved by the proposed ICP-ABE algorithm. The prevailing techniques like DH, RSA, ECC, and CPABE have the security of 88.2397%, 90.6845%, 92.834%, and 95.6234%, respectively. Furthermore, the ICP-ABE algorithm acquires more security than the other techniques.

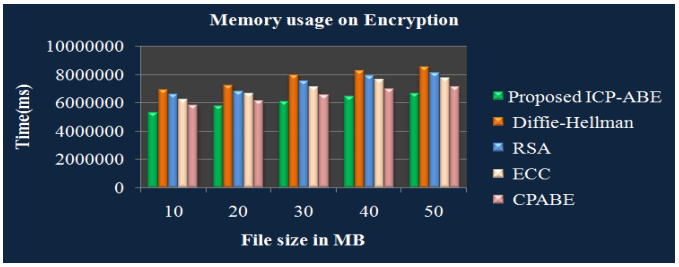

Fig.8. Memory usage on encryption

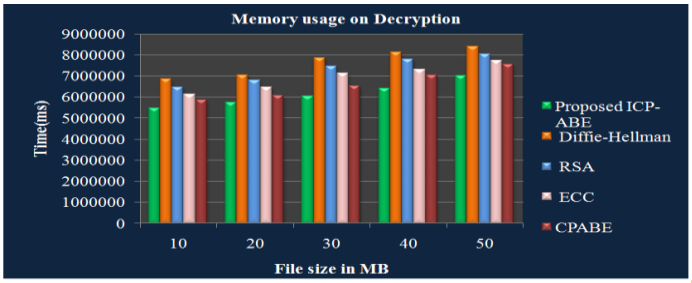

Fig 9. Memory usage on decryption

1). Analysis

Figure 8,9 portrays the pictorial depiction of memory usage of the proposed technique and prevailing methodologies on encryption and decryption. The proposed technique takes 5347845ms time on encryption and 5471145ms time on decryption for the file size of 10MB, wherein the prevailing methodologies take more time than the proposed technique. For the memory usage on encryption, the prevailing DH technique consumes more time for all file sizes. Regarding the memory usage for encryption and decryption, the comparison of the proposed technique with existing methodologies exhibit that the ICP-ABE technique consumes lesser time for the differing file sizes.

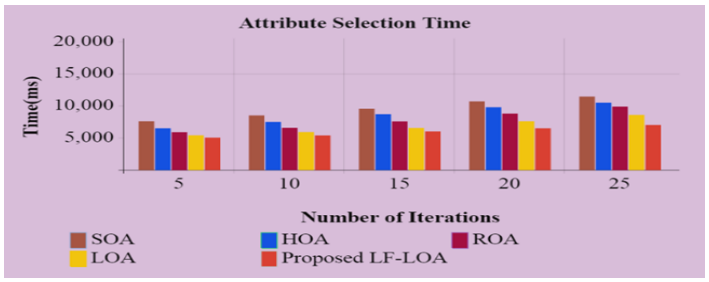

Fig.10.Grpahical representation for the attribute selection time of our proposed algorithm and the existing algorithms

E. Analysis

The attribute selection time of the proposed LF-LOA and the existent SOA, HOA, ROA, and LOA is displayed in figure 7. For the LF-LOA technique, the attribute selection time of 5 iterations is 5012ms. The prevailing techniques like SOA, HOA, ROA, and LOA have the attribute selection time of 7566ms, 6477ms, 5856ms, and 5367ms, respectively, for the same number of iterations. A medium attribution selection time has been attained by the technique ROA, which is lower than the SOA and HOA techniques and higher than the LOA and LF-LOA methodologies. It evinces that the LF-LOA method takes lesser time for the attribute selection than existent techniques when analogized to the leftover number of iterations.

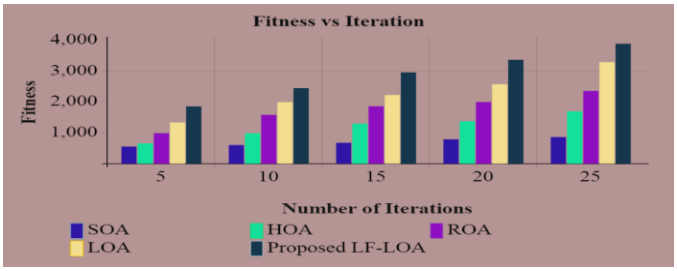

Fig.11. Fitness vs Iteration Analysis

1). Analysis

For the number of 5 iterations, figure 8 explicates that the proposed methodology has the fitness value of 1846 while the prevailing SOA, HOA, ROA, and LOA methodologies have the fitness values of 547, 648, 982, and 1324, respectively. For the rest of the iterations say 10, 15, 20, and 25 iterations, the LF-LOA technique has the fitness values of 2436, 2945, 3356, and 3874, respectively, which exhibits that the LF-LOA technique acquires a greater fitness value than other methodologies.

V CONCLUSION

An emerging concept of exchanging health information for research and other reasons is called the sharing of the personal EHR. Although patients and healthcare organizations are ready to share, it is still challenging on account of technical problems. Confidentiality, privacy, interoperability, integrity, etc are the technical obstacles. To improve the security in EHR data storage on a cloud platform, the ICP-ABE centered encryption scheme is utilized. EHR data collections, secure uploading, and secure downloading are encompassed in this research method. The attribute extractions, attribute selection, access policy creation, and secure uploading are entailed in the secure uploading phase. By utilizing the LF-LOA and ICP-ABE algorithms, the secure uploading process is carried out. The proposed technique's performance is perused by utilizing EHR data in an experimental evaluation. Regarding ET, DT, memory usage on encryption and decryption, and SL, the proposed ICP-ABE's performance is analogized to the existent CP-ABE, ECC, RSA, and DH algorithms. An SL of 95.62% is acquired by the proposed ICP-ABE, which is greater than the other techniques. Centered on attribute selection time and fitness versus iteration process, the LF-LOA's performance is weighed against the prevailing SOA, HOA, ROA, and LOA. When analogized to the other prevailing research techniques, the attribute selection time is also lower for the proposed LF-LOA. Therefore, the proposed technique-centered secure EHR uploading process achieves better performance than the top-notch methodologies. To save the memory usage in a hospital CS, the proposed method can be enhanced in the future by checking whether the same medical record will be uploaded, again and again, and initiating a new method to safely share the medical with other consulting doctors in some other hospital

REFERENCES

[1] Sheng Cao, Gexiang Zhang, Pengfei Liu, Xiaosong Zhang, and FerranteNeri, "Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain", Information Sciences, vol. 485, pp. 427-440,2019,10.1016/j.ins.2019.02.038J

[2] ShekhaChenthara, Khandakar Ahmed, Hua Wang, and Frank Whittaker, Security and privacy-preserving challenges of e-health solutions in cloud computing", IEEE access, vol. 7, pp. 74361-74382, 2019,10.1109/ACCESS.2019.2919982

[3] Afnan SalemBabrahem, and Muhammad MostafaMonowar, "Preserving confidentiality and privacy of the patient's EHR using the OrBAC and AES in cloud environment", International Journal of Computers and Applications, pp. 1-12,2018,10.1080/1206212X.2018.1505025

[4] LinglingXu, Zhiwei Sun, Wanhua Li, and Hongyang Yan, "Delegatable searchable encryption with specified keywords for EHR systems", Wireless Networks, pp. 1-13,2020, 10.1007/s11276-020-02410-3

[5] JayneelVora, PritItaliya, SudeepTanwar, SudhanshuTyagi, Neeraj

Kumar, Mohammad S. Obaidat, and Kuei-Fang Hsiao, "Ensuring privacy and security in e-health records", In 2018 International conference on computer, information and telecommunication systems (CITS), IEEE, pp. 1-5, 2018, 10.1109/CITS.2018.8440164

[6] IsmailKeshta, and AmmarOdeh, "Security and privacy of electronic health records: Concerns and challenges", Egyptian Informatics Journal, 2020,10.1016/j.eij.2020.07.003

[7] JayneelVora, AnandNayyar, SudeepTanwar, SudhanshuTyagi, Neeraj Kumar, Mohammad S. Obaidat, and Joel JPC Rodrigues, "BHEEM: A blockchain-based framework for securing electronic health records", in IEEE Globecom Workshops (GC Wkshps),IEEE, pp. 1-6, 2018,10.1109/GLOCOMW.2018.8644088

[8] HaoGuo, Wanxin Li, EhsanMeamari, Chien-Chung Shen, and Mark Nejad, "Attribute-based multi-signature and encryption for HER management: A blockchain-based solution", In IEEE International Conference on Blockchain and Cryptocurrency (ICBC),IEEE, pp. 1-5, 2020,10.1109/ICBC48266.2020.9169395

[9] Han-Yu Lin, and Yan-Ru Jiang, "A multi-user ciphertext policy attribute based encryption scheme with keyword search for medical cloud system", Applied Sciences, vol. 11, no. 1, pp. 63,2021

[10] Maithilee Joshi, KarunaPande Joshi, and Tim Finin Delegated authorization framework for EHR services using attribute based encryption", IEEE Transactions on Services Computing, 2019,10.1109/TSC.2019.2917438

[11] Vijayakumar, V, PriyanM. K, Gandhi Ushadevi, VaratharajanR, GunasekaranManogaran, and Prathamesh Vijay Tarare, "E-health cloud security using timing enabled proxy re-encryption", Mobile Networks and Applications, vol. 24, no. 3, pp. 1034-1045,2019

[12] KhaledRiad, RafikHamza, and Hongyang Yan, "Sensitive and energetic IoT access control for managing cloud electronic health records", IEEE Access,vol. 7, pp. 86384-86393,2019,10.1109/ACCESS.2019.2926354.

[13] Sood, Sandeep K, "A combined approach to ensure data security in cloud computing", Journal of Network and Computer Applications, vol. 35, no. 6, pp. 1831-1838,2012.

[14] Chinnasamy P and DeepalakshmiP, "Design of secure storage for health-care cloud using hybrid cryptography", InSecond International Conference on Inventive Communication and Computational Technologies (ICICCT), IEEE, pp. 1717-1720, 2018, 10.1109/ICICCT.2018.8473107.

[15] YangMing, and Tingting Zhang, "Efficient privacy-preserving access control scheme in electronic health records system", Sensors, vol18, no.10, pp. 3520,2018.

[16] Jiguo Li, Ningyu Chen, and Yichen Zhang, "Extended file hierarchy access control scheme with attribute based encryption in cloud computing", IEEE Transactions on Emerging Topics in Computing, 2019, 10.1109/TETC.2019.2904637

[17] AkshayTembhare, SibiChakkaravarthyS, SangeethaD, VaidehiV, and VenkataRathnamM, "Role-based policy to maintain privacy of patient health records in cloud", The Journal of Supercomputing, vol. 75, no. 9, pp. 5866-5881,2019.

[18] SiddheshMhatre, and Anant V. Nimkar, "Secure cloud-based federation for EHR using multi-authority ABE", In Progress in Advanced Computing and Intelligent Engineering,Springer, Singapore, pp. 3-15, 2019,10.1007/978-981-13-0224-4_1.

[19] KwangsooSeol, Young-Gab Kim, Euijong Lee, Young-DukSeo, and Doo-Kwon Baik, "Privacy-preserving attribute-based access control model for XML-based electronic health record system", IEEE Access, vol. 6, pp. 9114-9128, 2018,10.1109/ACCESS.2018.2800288.

[20] SeyedMortezaPournaghi, MajidBayat, and YaghoubFarjami, "MedSBA: A novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption", Journal of Ambient Intelligence and Humanized Computing,

pp. 1-29,2020,10.1007/s12652-020-01710-y.
[21] Xueyan Liu, Xiaotao Yang, YukunLuo, Li Wang, and Qiang Zhang, "Anonymous electronic health record sharing scheme based on decentralized hierarchical attribute-based encryption in cloud environment", IEEE Access, vol. 8, pp. 200180-200193,2020,10.1109/ACCESS.2020.3035468.
[22] SanaBelguith, NesrineKaaniche, Maryline Laurent, AbderrazakJemai, and RabahAttia, "Accountable privacy preserving attribute based framework for authenticated encrypted access in clouds", Journal of Parallel and Distributed Computing, vol. 135, pp. 1-20,2020,10.1016/j.jpdc.2019.08.014.
[23] GandikotaRamu, B. Eswara Reddy, AppawalaJayanthi, and LV Narasimha Prasad, "Fine-grained access control of EHRs in cloud using CP-ABE with user revocation", Health and Technology, vol. 9, no. 4, pp. 487-496,2019.
[24] Hao Wang, and Yujiao Song, "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain", Journal of medical systems, vol. 42, no. 8, pp. 1-9,2018.
[25] JayashreeGopalsamy and Dr.C. Priya," Data Integration with XML ETLProcessing", 2020, IEEE. https://ieeexplore.ieee.org/document/9132939
[26] Yi Liu, Yinghui Zhang, Jie Ling, and Zhusong Liu, "Secure and fine-grained access control on e-healthcare records in mobile cloud computing", Future Generation Computer Systems, vol. 78, pp. 1020-1026,2018, 10.1016/j.future.2016.12.027.
[27] S.Prathima, Dr.C.Priya, "Privacy and Security Implementation in Existing Cloud Based Electronic Health Records – A Detailed Review" in International Journal of Advanced Science and Technology, Vol 29, Issue No.7, June 2020, pp2844-55
[28] S.Prathima, Dr.C.Priya," Privacy Preserving and Security Management in Cloud based Electronic Health Records -A Comprehensive Study", Singapore, Springer, 2020 https://link.springer.com/chapter/10.1007/978-981-15-3284-9_9
[29] SheelaKasinathan and Dr.C. Priya," Enabling The Efficiency Of BlockchainTechnology In Tele-Healthcare With Enhanced EMR", 2020, IEEE. https://ieeexplore.ieee.org/document/9132922