JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 2102-2120
https://publishoa.com
ISSN: 1309-3452

A Secure EHR Protection Strategy by Hybrid Encryption Scheme with Permissioned Blockchain

Ms. Nilima V. Pardakhe[1], Dr. V. M. Deshmukh[2]

Research Scholar[1], Associate Professor[2]
Department of Computer Science & Engineering[1 2]
Prof. Ram Meghe Institute of Technology & Research, Badnera[1 2]
pardakhenilima@gmail.com[1],vmdeshmukh@mitra.ac.in[2]

Abstract

Background: The digitization of conventional medical information makes medical institutions suffer from some challenges in storing and sharing Electronic health records (EHRs). Accessing the patient's medical history is significant for appropriately prescribing the medication.

Objectives: The major aim of the paper is to implement a hybrid meta-heuristic-based Ciphertext Policy-Attribute-based encryption (CP-ABE) based on permissioned blockchain to ensure data confidentiality and access control of medical data

Methods: Here, the hybrid algorithm is developed called Hybrid Deer Grasshopper Hunting Optimization (HGHO), which is used to perform the attribute optimization in CP-ABE. Hence, the ciphertext size, the encryption cost, and the communication cost are reduced through the optimization concept.

Conclusions: Finally, the performance evaluation confirms the proposed scheme's reliability and robustness compared to existing standard constructions**.**

Keywords: Electronic Health Records Protection Strategy; Permissioned Blockchain; Ciphertext Policy-Attribute-based encryption; Hybrid Deer Grasshopper Hunting Optimization; Secured Healthcare System

1. Introduction

EHRs are used to reduce the cost inefficiency of conventional medical data storage systems. It is developed to allow the patients to maintain their medical data. Data users are enclosed with restricted access to the EHRs [9]. At the same time, the patients cannot share their medical data among the data users, which indicates the privacy and safety of the EHR for the patient's data. On the aspect of using EHRs, an encrypted format for retrieving these records needs to be developed [10]. The enhancement was made in the EHRs to extend the attention of the distributed storage platforms with the different storage devices. These storage platforms become enlarged in numbers, so the distributed platforms are aimed at cyber attacks as they store the data [11]. Specific applications related to big data for supporting the health care medications and services are usually handled with the third parties or the public for surveying

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 2102-2120
https://publishoa.com
ISSN: 1309-3452

and acquiring the essential reports [12]. In specific scenarios, the data records of the sensitive patients are undergone malicious attacks, and the risks are enclosed with the processes like unauthorized access and tampering. Hence, it is necessary to rectify a problem to ensure privacy and security during system design to preserve sensitive healthcare data [13]. Healthcare and other systems are involved with specific protection requirements such as integrity, data storage, secure transmission, privacy-based authentication, and tamperproof monitoring [14].

Blockchain is considered the new technology for enhancing healthcare systems' security and privacy levels [15]. Owing to the immutable feature of the blockchain, e-healthcare data is preserved in the secured medical blocks for asserting privacy and data integrity [16]. As the blockchain is enclosed with a decentralized nature, it is used for achieving a certain level of security independent of another intermediary [17]. Efforts have been made to integrate the blockchain to design the IoT systems to achieve smart cities and homes [18]. On the other hand, when considering the healthcare settings, the data sources of the EHRs are incorporated with the different unstructured and structured data types like image and text that are effectively large and also impractical for transmitting the data among the conventional wireless network systems. Blockchain is classified into three significant types: consortium, private, and public [19]. A public blockchain allows any stakeholder like users and miners to access the transactions and blocks in the network. The private blockchain is involved with the necessary stakeholders to grant the prior consent for combining the blockchain and becomes more limited. At last, the consortium blockchain is appropriate for huge business applications or enterprises, in which a set of people can able to revoke or grant access to the blockchain [20].

Privacy-preserving methods protect the confidential and original data accessed by unauthorized third parties [21]. The main intention of these methods is to conceal, distribute, convert and alter sensitive information like EHRs of the healthcare systems that needs to be prevented with the breach of original data at the time of processing with the third-party systems [22]. Every task in the healthcare sector seems to be difficult concerning the time and processing to insert the EHR into the system. Providers are faced with various struggles to store, secure, and verify health records as it has a huge volume of health records of diverse types. When retrieving the preserved health record with high quality under the crucial conditions becomes challenging in the health sector [23]. Interoperability is the most critical challenge in the healthcare industry, and the health records that have been exchanged among the providers are also considered a significant task. In designing a new system for overcoming these barriers, the system must include the constraints for securing the EHRs rather than considering the fast retrieval, adequate storage, secure the data sharing across the providers, and managing the patient-provider relationships [24]. The healthcare domain needs to secure the private data of the patients. It is failed to preserve the integrity and privacy of health data like scan reports, drug details, microbiological test reports, prescriptions, treatment history, disease details, and patient personal data [25]. However, a private blockchain is known as the permissioned blockchain, in which the registered participants can access the network. Additionally, the conventional blockchain solution for medical data retrieval does not provide detailed solutions for data users and

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 2102-2120
https://publishoa.com
ISSN: 1309-3452

owners. Hence, there is necessary to develop a new blockchain-aided healthcare management data model.

The essential improvements to the suggested model are described below.

- To build a new permissioned blockchain-based EHR security model for protecting and securely accessing patients' health records to avoid the confidentiality loss and integrity loss of the patient's data with the help of CP-ABE and optimization techniques-aided encryption on the data transmission.

- To implement the enhanced CP-ABE approach for encrypting the healthcare data with a heuristic-based optimal key to secure and protect the healthcare data transmission by accessing with the authorized users or doctors, or patients.

- To introduce a hybrid heuristic strategy named HGHO for choosing the optimal encryption key for providing high security to the health data transmission by reducing the ciphertext size, computational cost, and encryption cost in the proposed model.

- To evaluate the efficiency of the proposed permissioned blockchain-based EHR security model by evaluating its convergence, encryption time, and decryption time.

The rest of the parts are reviewed as follows. Part II discusses the earlier studies on associated EHR security models and their limitations. Part III shows the permissioned blockchain-based EHR security model. Part IV describes the CP-ABE approach for data encryption and develops the HGHO algorithm. Part V explains the algorithm description and the retrieval procedure for medical records. Part VI describes the acquired results and their interpretations. Part VII concludes the developed model.

2. Literature Survey

2.1 Related Works

In 2020, Zhuang *et al.* [1] have ensured a feasible solution for healthcare data management with the help of unique features presented in the blockchain, where a distributed ledger technology was involved as it was "unhackable." With the intelligent contract feature, it was inserted as the programmable self-executing scheme into the blockchain. This was developed to protect the privacy and security of the data and the patient's privacy, which was also responsible for providing complete access to their healthcare records. Huge-scale simulations were performed with the patient-centric health information to evaluate the model's "feasibility, stability, security, and robustness."

In 2020, Niu *et al.* [2] implemented a healthcare data sharing method according to the permissioned blockchains. The ciphertext was utilized for attribute encryption to ensure access control and data confidentiality over the medical data. Here, a polynomial equation was incorporated to provide the privacy of a patient's identity to attain the arbitrary association of keywords, and then, the blockchain technology was correlated. Moreover, the developed method has shown better retrieval efficiency than the conventional techniques, which was observed through the evaluation.

In 2021, Ray *et al.* [3] developed a new methodology named BIoTHR for ensuring privacy based on the blockchain and swarm exchange approaches for facilitating the secure and seamless transmission of user data within

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 2102-2120
https://publishoa.com
ISSN: 1309-3452

the secured nodes over the peer-to-peer communications. The proposed scheme was implemented with the IoT on the EHR management based on the private blockchain. Swarm exchange infrastructures and blockchain were introduced for the developed scheme to ensure reliable and secure data transmission. The analysis was made in the proposed scheme to show the high efficiency with the swarm exchange, blockchain-IoT, and EHR transmission than some of the peer techniques.

In 2019, Rajput *et al.* [4] have integrated the "Emergency Access Control Management System (EACMS)" according to the hyperledger composer and hyperledger fabric of the permissioned blockchain. The developed system has described several rules based on the smart contracts to handle the emergencies and duration of time for the emergency access of healthcare data, which has been assigned with certain restrictions for accessing it by the patients. The efficiency was evaluated for the suggested framework by implementing a hyperledger composer based on accessibility, security, privacy, and response time.

In 2022, Tan *et al.* [5] developed a blockchain-assisted privacy and security protection method named "Decision Bilinear Diffie-Hellman (DBDH)" for direct revocation of medical records related to COVID-19 based on the encryption with the cipher policy attribute. Here, the blockchain was used to perform the uniform identity authentication, and the entire public keys were stored in the blockchain. The role of the system manager was to generate the parameters of the system and publish the private keys to the users and medical practitioners. The analysis has revealed that the developed model has secured significantly less overhead in storage and communication than other baseline schemes.

In 2022, Chelladurai and Pandian [6] implemented an intelligent contract-based blockchain technology to provide a promising solution for the requirements of health service providers, physicians, and patients. The developed system has focused on exchanging health information through the blockchain platform for constructing the intelligent e-health system. The implemented system has introduced the health models based on the "Modified Merkle Tree data structure" for providing secured storage facilities and fast access to healthcare data among diverse providers. The quantitative and qualitative measures were computed for the developed system to evaluate the efficiency of the resources, transaction latency, and the transactions per second.

In 2020, Nagasubramanian *et al.* [7] have incorporated the confidentiality loss for making the passive impact on securing the health records. It was a basic necessity to preserve the EHR. Health data was confirmed by developing a system-aided with the cloud for ensuring the authentication and efficiency in providing the integrity of the health records. Here, the data integrity was controlled with the developed technology of blockchain. The effectiveness of the developed framework was verified using several parameters such as cost, average time, size of data retrieval, and storage over the blockchain technology.

In 2020, Dagher *et al.* [8] have suggested a new model with the blockchain to secure, efficient and interoperable access for the medical records with the third parties, providers, and patients at the time of privacy preservation of the sensitive information of the patients. The developed approach named ancile is integrated based on the smart contracts to enhance access control and data obfuscation by incorporating the

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 2102-2120
https://publishoa.com
ISSN: 1309-3452

superior cryptographic approaches to improve security. The main intention of the work was to evaluate the proposed framework's interaction with the diverse requirements of the patients and further learn the addressing strategy of security and privacy concerns in the healthcare sectors.

2.2 Problem statement

Existing EHRs using blockchain systems are reviewed in Table 1, with several features and challenges. Smart contract [1] has ensured robustness, security, stability, and feasibility efficiency. This model has offered superior generalization ability. On the other hand, this model requires setup at every healthcare facility. Ciphertext-based attribute encryption [2] has achieved excellent retrieval efficiency and ensures the reliability and authenticity of the uploaded data. However, the proposed model gets lower search efficiency. BIoTHR [3] protects patients' data privacy and offers low cost and high availability. This model does not utilize lightweight IoT devices. EACMS [4] guarantees maximum performance regarding accessibility, security, privacy, and response time. This model has offered superior efficiency when compared to conventional medical systems.

Conversely, it needs higher memory. DBDH [5] maximizes the performance regarding delay and throughput and provides superior security. However, this model suffers from real-time attacks. Modified Merkle Tree data structure [6] achieves efficiency in transaction latency, transactions per second, and resources. The performance analysis of the designed model is ensured concerning resource utilization, delay, transaction response time, and throughput. However, the system's latency increases while increasing the number of participants. Timestamped algorithm [7] ensures the security of sensitive health data and takes less time than the existing models. However, this model does not process and offers privacy to the small data chunks. Smart contracts [8] provide security and access control and prove higher data integrity and privacy preservation. This model is not applicable for intelligent contracts with large local databases. This review will help the researchers suggest a new EHR model through blockchain.

3. System Model of EHR

The enhancement in medical data safety is made by developing the proposed method on the medical platform, as given in Fig. 1. According to the medical institutions, they have shared the information in particular regions. The doctors usually store the encrypted EHRs over the servers of their corresponding hospitals. The administrator of the servers has to focus on preserving specific keywords in the permissioned blockchain for achieving EHRs sharing between the hospitals. The six different attributes of the system model are explained below.

System Manager: The system manager is responsible for the entire system, and also it is necessary to enroll through the registration of data users, doctors, and every patient before they are entering into the system. These system managers generate the private and public keys for data users. Moreover, the system managers are usually distributed and revocating the attribute, acting as the attribute authority.

EHR system: This attribute is regarded as the users who ensure the medical services for the medical institutions. Mostly, every hospital has its server along with different computer clients. These clients are used for recording the health information of the patients. The server

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 2102-2120
https://publishoa.com
ISSN: 1309-3452

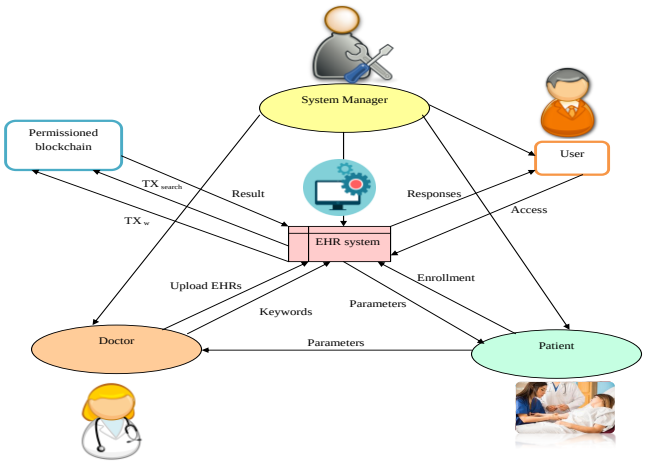
generally enrolls the doctors and users in the system. The server administrator is used to broadcast the keywords related to EHRs to the permissioned blockchain. When uploading the EHRs by the doctors to the server, the server needs to verify the doctor's identification.

Patient: The patient's registration must be done when visiting a hospital for the first time. In the registration phase, the patients will be given the visit token that acts as a pass for the patient to consult the doctor. The authorized doctor is used for generating an EHR of the patients and preserved as the encrypted EHR over the hospital server. The server manager is used for storing specific keywords of EHRs on the permissioned chains.

Doctor: The doctors are used to produce the EHR of the patients and perform the encryption of EHR with the access structure of the patient. Further, it needs to be uploaded by the doctor into the EHR system as the encrypted EHR.

Data User: When the data users or third-party organizations need to access the patient data other than the patient or hospitals, it is compulsory to have the searching trapdoors produced by the patients for performing the keywords searching in the field of blockchain.

Blockchain: The involved users in the permissioned blockchain are enclosed in the medical institutions, and the searchers are comprised of the participants mentioned through the permissioned blockchain system. Participants are verified with the transaction records broadcast through every server towards the blockchain and have implemented the data search function over the permissioned blockchain. The EHR system model is diagrammatically represented in Fig. 1.



System model for EHR

3.1 Permissioned Blockchains

Public chains are termed blockchains, in which everyone can access the system at all times when it requires reading data, sending transactions, and competing for accounting. Public chains encourage the participants to compete to account for the data through the encryption of digital currencies like Ethereum and bitcoins to ensure data security. Public chains are entire of a decentralized nature. Permissioned blockchains allow the full participants node as the permission node over the blockchain system that may be alliance and private chains. Several permissioned blockchains are comprised without any digital

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 2102-2120
https://publishoa.com
ISSN: 1309-3452

currency strategy due to specific nodes being enclosed for processing independent of requirements for the currency encryption in the system. The nodes in the permissioned chain are used for performing some functions like writing, accessing, and reading information on the blockchain. There is an increasing business count employing the permissioned blockchain networks as these networks undergo configuration. This network is involved with the required restrictions and manages the roles where all the participants are necessary for processing all the applications. The storage capacity of the medical information and the way determining the participants over the permissioned chain are diagrammatically represented in Fig. 2.

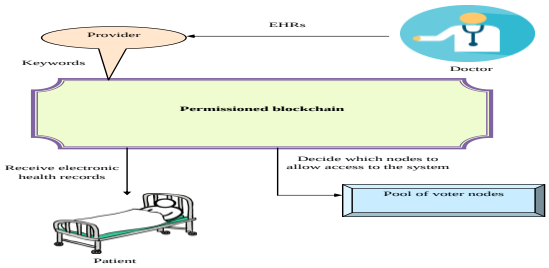


Fig. 1. Data storage model on permissioned blockchain

4. Methodology

4.1 CP-ABE Model

Access control methods effectively provide authorized users access to the medical data in the EHR system. Though there are many access control methods, ABE is efficient in many domains. It has high efficiency in offering the appropriate-grained access control, providing the security with complex collusion resistance, and reducing the overhead problems in the communication. However, it comprises many difficulties in implementing the complex access control policies and does not permit the users to perform the decryption without checking the authorization. Hence, CP-ABE is developed with the ciphertext policy, an access framework over the ciphertext. This method gives the EHR system high confidentiality over the data even performed with the untrusted storage server. The CP-ABE approach encrypts the message with the data owner, which is incorporated with a particular access policy in the ciphertext and permits the authorized users to perform the data decryption. Therefore, the data access control is conducted with the help of CP-ABE, where the attributes are considered with certain authorities by the users. The data owners make the distribution of data using the access policy shown with the attributes through several authorities. The user's attributes are changed dynamically, and users construct some new attributes, and the alteration of data access needs to be done simultaneously. The entire data owner separates data into several parts prior to the data encryption, where all the parts have undergone encryption with content keys.

Moreover, the data owner interprets the access policies with the help of some authorities from the attributes and the content keys for policies encryption. Following data encryption, it is passed towards the cloud servers using ciphertext. But, the servers are not permitted to access the health records. Then, the data

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 2102-2120
https://publishoa.com
ISSN: 1309-3452

decryption occurs with the users when satisfying the user attributes with the access policy mentioned in the ciphertext.

4.2 Meta-heuristic-based CP-ABE

Most of the existing multi-authority CP-ABE approaches are provided better performance, but it faces challenges when policies are offered with a single set by the users. Hence, the data is protected by the data owner in this proposed model. Information retrieval is performed with the data users from the cloud using blockchain technology and smart contract options. Cloud computing is offered high security over healthcare data with the support of an enhanced CP-ABE approach, which is enhanced with the proposed HGHO algorithm. The proxy server is considered the server where the encryption and decryption of data occur with the files using the secret key. The access control is further advanced by involving the blockchain transactions and the smart contracts that make the access records over the blockchain tamperproof and auditable. The smart contracts are employed to accomplish mutual trust between the authorities and collect the attribute sub-tokens to perform the collaborative computations to produce the decryption tokens for the users. This heuristic-based CP-ABE approach gets the input as the plain text for securing the data through the optimal key-based encryption and decryption. Here, the developed HGHO is utilized to tun the optimal keys to ensure the security of the data transmission over the data owners and data users. The main focus for performing the optimal key generation with the proposed algorithm is to attain less computation cost Cs, encryption cost, Ec and ciphertext size Cts, as given in Eq. (1).

$$Oj = \arg\min_{\{Sk\}} \left[Cs + Ec + Cts \right] \quad (1)$$

Here, the term Sk is indicated as the generated optimal secret key.

4.3 Proposed Algorithm

The developed permissioned blockchain-based secured EHR model introduces the HGHO to choose the optimal key for encrypting medical text data to make a highly secured EHR in medical institutions. GOA [26] is used in the developed model due to its improved efficiency in determining the optimal solution and not undergoing the optimum local problem. But, this model cannot solve different optimization problems as the search agents usually achieve their comfort regions at high speed, making it less convergence at a similar point. Therefore, the DHOA [27] is adopted into the GOA, named HGHO, to obtain the perfect solution for the security problem in EHR transmission. The developed HGHO is enclosed with the deviation-based concept for updating the final position of candidates to obtain the optimal solution. First, the GOA deviation is estimated with "the solution in GOA without any computations that are represented by dv_1." Similarly, the DHOA deviation is computed and expressed dv_2 without any computation in the DHOA. The final position upgrade is taken place as shown in Eq. (2).

$$Pos = Pos + dv_1 + dv_2 \quad (2)$$

In Eq. (10), the current position of the solution is indicated by Pos, and the best solution is depicted as Bst.

GOA [26] is implemented with the characteristic features of a grasshopper with three different functions such as "target seeking, exploration, and exploitation." The characteristic features of the grasshoppers are

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 2102-2120
https://publishoa.com
ISSN: 1309-3452

used to updat Xt_r r^{th}e the solution's position as in Eq. (3).

$$Xt_r = St_r + Gt_r + At_r \tag{3}$$

The gravity force of the r^{th} solution is termed to be Gt_r the wind advection is shown by At_r. The randomly determined features are computed as shown in Eq. (4).

$$Xt_r = Rh_1 St_r + Rh_2 Gt_r + Rh_3 At_r \tag{4}$$

Here, the random numbers are expressed by Rh_1, Rh_2 and Rh_3. Then, the social interaction is depicted St_r, computed in Eq. (5).

$$St_r = \sum_{\substack{jt=1 \\ jg \neq ig}}^{Nt} sT\left(dT_{rjt}\right)\widehat{dT}_{rjt} \tag{5}$$

Here, the distance between two solutions is described dT_{rjt}, the unit vector computed from r^{th} solution to the jt^{th} solution is depicted $\widehat{dT}_{rjt} = \dfrac{xT_{jt} - xT_r}{dT_{rjt}}$, and the function that influences the social force is represented sT. The component Gt is estimated with Eq. (6).

$$Gt_r = -gT\hat{e}_{gT} \tag{6}$$

Here, the term $\hat{e}_{gT}$ denotes the dimension's unity vector and similarly gT expresses the gravitational constant. The component At is determined with Eq. (7).

$$At_r = uTe\widehat{T}_{wT} \tag{7}$$

The unit vector is depicted $e\widehat{T}_{wT}$ in the winding path, and the constant drift is described uT. Further, Eq. (3) can be replaced and depicted as Eq. (8).

$$Xt_r = \sum_{\substack{jt=1 \\ jt \neq it}}^{Nt} sT\left(\left|xT_{jt} - xT_r\right|\right)\frac{xT_{jt} - xT_r}{dT_{rjt}} - gT\hat{e}_{gT} + uTe\widehat{T}_{wT} \tag{8}$$

Here, the grasshopper count is depicted Nt, and the social force is indicated $sT(rT) = fTe^{\frac{-rT}{lT}} - eT^{-rT}$. This mathematical model cannot solve the optimization challenges directly, so it is modified as Eq. (9).

$$Xt_r^{dT} = cT\left(\sum_{\substack{jt=1 \\ jt \neq it}}^{Nt} cT\,\frac{up_{dT} - lp_{dT}}{2}\,sT\left(\left|xT_{jt}^{dT} - xT_r^{dT}\right|\right)\frac{xT_{jt} - xT_r}{dT_{rjt}}\right) + T\hat{t}_{dT} \tag{9}$$

Here, the term cT is indicated as the decreasing coefficient that minimizes the comfort zone of the algorithm that is proportional to its iteration counts, and the lower and upper bound of the solution are correspondingly represented by up_{dT} and lp_{dT}.

DHOA [27] is implemented with the hunting strategy of the humans towards the deer, which is based on the hunter's behavior. Here, the best solution is updated Xt^{sp} Xt^{lp}, regarded as the successor and leader positions, respectively. Similarly, the position angle-based update in the DHOA is shown below.

(1) "Propagation based on leader's position": Here, the encircling of the deer happens with their encircling behavior, and it is used for reaching the best position as in Eq. (10).

$$Xt_{y+1} = Xt^{lp} - Fi \cdot hi \cdot \left|Zi \times Xt^{lp} - Xt_y\right| \tag{10}$$

The random variable hi that lies in the interval $[0,2]$ and wind speed is expressed Fi, and the coefficient vector is denoted Zi. The position of

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 2102-2120
https://publishoa.com
ISSN: 1309-3452

the solution at the current iteration is represented by Xt_y, and the position for the nest iteration is depicted by Xt_{y+1}. At the starting stage, the position of the hunter is indicated (Xt, Au). After the position update, the best position is expressed (Xt^*, Au^*), which changes according to the coefficient vectors Fi Zi. If the condition $(hi < 1)$ is satisfied, then the position is updated with Eq. (10), or else, the position angle or successor position is used for position updating.

(2) "Propagation based on position angle": The position angle is determined by knowing the hunter's position. The next iteration of the position angle is shown in the Eq. (11)

$$Xt_{y+1} = Xt^{lp} - hi \cdot \left|\cos(u) \times Xt^{lp} - Xt_y\right| \quad (11)$$

Here, the term hi denotes the random number and Xt_y^* represents the best position.

(3) "Propagation based on the successor position": The vector Zi determines the updating position of the hunter. If the vector Zi s are below 1, modify the position according to the successor position as in Eq. (12).

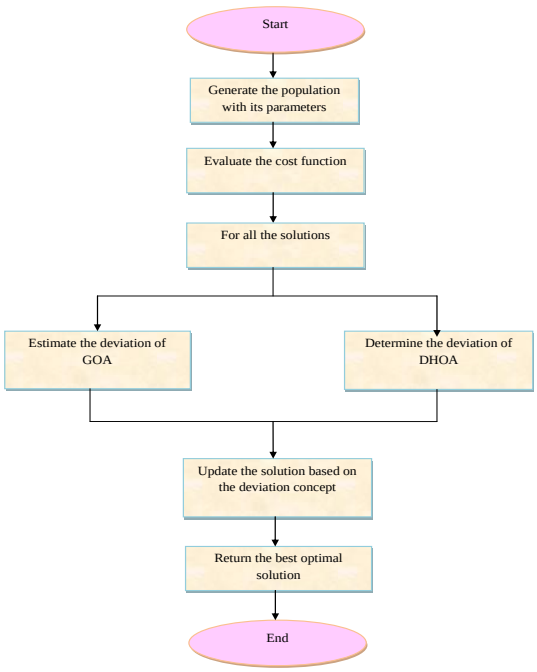
$$Xt_{y+1} = Xt^{sp} - Zi \cdot hi \cdot \left|Zi \times Xt^{sp} - Xt_y\right| \quad (12)$$

The pseudo-code of the proposed HGHO is given in Algorithm 1. Here, the successor position of the hunter is depicted Xt^{sp}. Then, determine the fitness value for every search agent and update both the leader and successor position until the stopping condition is satisfied. Finally, the best solution is attained. The flowchart of the proposed HGHO is given in Fig. 3.

Algorithm 1: Proposed HGHO

```
Generate the initial population and its parameters
Calculate the fitness function of every solution
While (stopping condition)
  For each
    Position update based on the GOA using Eq. (9)
      Determine the deviation dv1 of GOA
    Update the position of the solution using DHOA
      Upgrade the position with Eq. (10) when (hi < 1)
      Upgrade the position with Eq. (11) when (hi ≥ 1)
      Compute the deviation dv2 of DHOA
    End
    Update the final solution using Eq. (2).
  End for
Update the parameters
End while
Obtain a best optimal solution
```

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 2102-2120
https://publishoa.com
ISSN: 1309-3452



5. Flowchart of the Proposed HGHO

The EHR sharing scheme is involved on the permissioned blockchain enclosed with different steps and six different algorithms as given below.

System Initialization:

$\text{Setup}(\lambda) \rightarrow (Pu, Sk)$: Here, the setup algorithm is processed with the help of the system manager. The input is obtained as a security parameter λ, and the output is given as the master secret key Sk and public parameters Pu.

Key Generation:

$\text{KeyGen}(Sk, Pu, Su) \rightarrow TK$: Here, the secret key generation algorithm is involved and controlled by the system manager. The input is acquired as the attribute set Su of a user, public parameters, Pu and master secret key Sk. Similarly, the output is regarded as the secret key TK.

Data Storage:

$Enc(Pu, S, U, N) \rightarrow (J, D)$ Here, the encryption algorithm is used, which the doctor handles. The EHRs N, keywords set U of shared EHRs, access control structure S of the patient Pt, and public parameters Pu are used as the input for the algorithm. The output is accomplished to be a ciphertext D and keywords index J.

Data Query:

$\text{Trapdoor}(Pu, U', TK) \rightarrow S_{U'}$ The user is employed to handle the trapdoor generation algorithm. The input is acquired as the secret key TK, search keywords set, U' and public parameters Pu, and the algorithm's output is attained as the search trapdoor $S_{U'}$.

$\text{Search}(J, S_{U'}) \rightarrow D$: Here, the search algorithm is processed with the support of participants, who are presented in the permissioned blockchain.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 2102-2120
https://publishoa.com
ISSN: 1309-3452

Here, the input is acquired as the search trapdoor $S_{U'}$ and keywords index J, and the output is received as the ciphertext D.

Data Decryption:

$\text{Decrypt}(Pu, Sk, D) \to N$: The user is accessed with the decryption algorithm with the input as ciphertext D, secret key, Sk and public parameters Pu. Finally, the decryption algorithm provides the message N as the output.

a. Process Carried out for Retrieval of EHR using Permissioned Blockchain.

The developed method has three stages: "system setup, data generation and storage, and data search and access."

***Stage 1-System setup*:**

- $\text{Setup}(\lambda)$: The input is given as the security parameter λ and considered the two different multiplicative cyclic groups such as H_1 and H_2 along with the generator q and the two generators of H_1 being denoted as h_1 and h_2. Assume it $f : H_1 \times H_1 \to H_2$ to be an admissible bilinear map. The system has chosen the variables $\alpha, \beta \in A_q^*$ and has computed $h_2^{\alpha}, h_2^{\beta}, h_2^{\frac{\beta}{\alpha}}$ them. Then, the four different functions are chosen as $I_1 : \{0,1\}^* \to A_q^*, I_2 : H_1 \to A_q^*$ $I_3 : A_q^* \to H_2$ and $I_4 : H_2 \to \{0,1\}^*$. The system parameters are described as $Pu = \left(q, f, h_1, h_2, h_2^{\alpha}, h_2^{\beta}, h_2^{\frac{\beta}{\alpha}}, H_1, H_2, H_3, H_4 \right)$ is used, and the master secret key Sk is generated with a secret as in Eq. (13).

$$Sk = (\alpha, \beta) \quad (13)$$

- $\text{KeyGen}(\lambda)$: Here, the system manager takes the responsibility of choosing $s \in A_q^*$, and the computation $S = h_1^{\frac{\alpha - s}{\beta}}$ $S' = h_1^{\frac{\alpha}{\beta}} h_2^{\frac{\alpha}{\beta} s}$ is done. The selection $u_b \in A_q^*$ is made for all attributes $b \in T$ and further determine $Y_b = h_1^{u_b}$ d $Z_b = h_1^{s} h_1^{u_b I_1(b)}$. Finally, the attribute authority passes the secret key TK towards the users as in Eq. (14).

$$TK = (S, S', \{Y_b, Z_b\} \forall b \in T) \quad (14)$$

Stage 2: "Data generation and storage"

The patient Pt visits the hospital to treat their illness, which the hospital server has randomly chosen $i \in A_q^*$ and has computed $\mu = I_3(i)$, and the server has reserved μ. Here, the term i is the secret key between the doctor E and patient during the consultation. The doctor E s are responsible for handling the encryption algorithm as given below.

- $Enc(n, v)$: In the first step, the doctor E has produced the health records $N \in \{0,1\}^*$ related to the patient Pt and has utilized the assessment structure (Γ, i) for computing $D_0 = h_1^{\frac{\beta i}{\alpha}}$ $D_1 = N \cdot I_4\left(f(h_1, h_1)^i\right)$. In the second step, the doctor is involved in extracting the keywords sets $b, c \in A_q^*$ for designing the polynomial equations according to the keyword $U = \{u_1, u_2, \ldots, u_n\}$ s given in Eq. (15).

$$\begin{aligned} h(y) &= b(y - I_1(u_1))(y - I_1(u_2)) \ldots (y - I_1(u_n)) + c \\ &= b_n y^n + b_{n-1} y^{n-1} + \ldots + b_1 y + b_0 \end{aligned} \quad (15)$$

Here, for every b_k, $k \in \{1,2,\ldots,n\}$ is used for computing $M_k = h_2^{\alpha b_k}$, $G_0 = h_2^{i} h_2^{c}$ and $G_1 = h_2^{\beta i}$. The

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 2102-2120
https://publishoa.com
ISSN: 1309-3452

output of the encryption algorithm is shown in Eq. (16) and Eq. (17).

$$D_N = (\Gamma, D_0, D_1) \quad (16)$$

$$J_u = (M_k, G_0, G_1, (B_w, C_w)_{w\in\Gamma}) \quad (17)$$

The doctor E uploaded the ciphertext D_N and J_u into the database server of the EHR system present in the hospital. After uploading the data, the cloud server needs to be verifying the authentication of a doctor. The doctor E has arbitrarily selected $s_1, s_2 \in A_q^*$ every attribute $b \in T$ and has $u_b^{'} \in A_q^*$ computed $\eta_1 = h_2^{s_1,s_2} h_2^{u_b^{'} I_1(b)}$ and $\eta_2 = h_2^{s_2 u_b^{'}} h'$. Then, the doctor transmits (η_1, η_2, i') it to the EHR server used $i^* = I_2\left(\frac{\eta_1}{I_1(b)}\right) \oplus i'$ and also has determined $I_3(i^*)$ to be true or not. Then, the correctness is given in Eq. (18).

$$\begin{aligned} I_3(i^*) &= I_3\left(I_2\left(\frac{\eta_1}{I_1(b)}\right) \oplus i'\right) \\ &= I_3\left(I_2\left(\frac{h_2^{s_1,s_2} h_2^{u_b^{'} I_1(b)}}{h_2^{u_b^{'} I_1(b)}}\right) \oplus i'\right) \\ &= I_3\left(I_2\left(h_2^{s_1,s_2}\right) \oplus i'\right) \\ &= I_3(i) = \mu \end{aligned} \quad (18)$$

The manager present in the EHR system is involved in extracting the block JE_c, which is the identification of the hospital, and the secure keyword indicate JE_{Pt} s the patient identity is expressed J_u. The server in the EH system is used to broadcast the new transactions towards the blockchain denoted by $UY_{J_u} = (JE_c, JE_{Pt}, J_u)$.

Stage 3: "Data search and access"

- Trapdoor: The trapdoor $S_{U'}$ belongs to the keyword set is indicated as in Eq. (19).

$$S_{U'} = \left(L_0, L_1, F_j, (Y_b', Z_b') \middle| b \in T\right) \quad (19)$$

- Search: The searcher is performed with the attributes on the permissioned blockchain belonging to a trapdoor and has computed the secret value of the leaf node as in Eq. (20).

$$F_w = f(h_1, h_2)^{ss_3 i_w(0)} \quad (20)$$

- Decrypt The data user has obtained the ciphertext $\mathrm{D} = (\mathrm{U}, \mathrm{D}_0, \mathrm{D}_1)$ through the hospital server, and the ciphertext's decryptions are performed with the ciphertext.

$$F_w' = \frac{f(Z_b, B_W)}{f(Y_b, C_W)} = f(h_1, h_2)^{si} \quad (21)$$

$$N = \frac{D_1}{I_4\left(\frac{f(S', D_0)}{F_w'}\right)} \quad (22)$$

The above two equations show the decryption of medical records for regaining the data related to the patients.

5. Results

5.1 Experimental setup

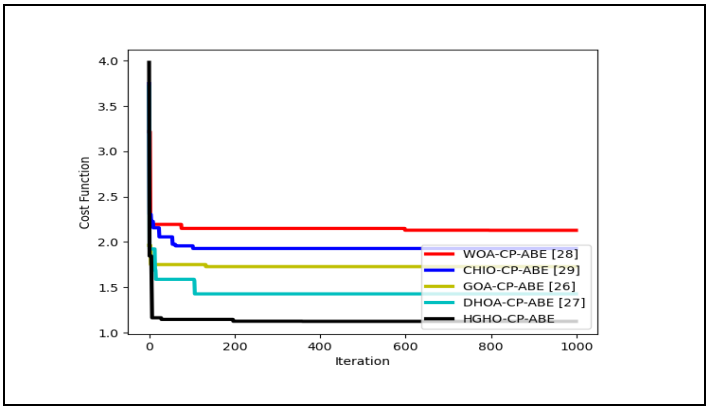
The permissioned blockchain-based secured EHR model is developed in Python, and further analysis was conducted to verify the transactional latency, time taken, and effectiveness of the system. The evaluation was made between the developed and state-of-the-art methods to improve the blockchain-based EHR transmission model. The population size of 10 and the maximum count of iterations of 1000 were utilized in the developed model. The proposed HGHO-CP-ABE was distinguished

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 2102-2120
https://publishoa.com
ISSN: 1309-3452

from other existing algorithms like " Whale Optimization Algorithm (WOA) [28], Coronavirus Herd Immunity Optimization (CHIO) [29], GOA [26] and DHOA [27], and machine learning algorithms like BIoTHR [3] and EACMS [4]".

5.2 Convergence analysis

The proposed HGHO-CP-ABE-based EHR transmission model secures less ciphertext size, computation cost, and encryption cost by tuning the encrypted keys for encryption and decryption, which is observed compared with conventional optimization techniques. The convergence rate of the proposed model is evaluated with different existing algorithms at the increasing iterations, as depicted in Fig. 4. The betterment of the proposed model is observed to be 14.2%, 13.3%, 12.02%, and 12.4% enhanced than WOA-CP-ABE, CHIO-CP-ABE, GOA-CP-ABE, and DHOA-CP-ABE, respectively at the 400^{th} iterations. Hence, it is verified that the suggested HGHO-CP-ABE-based model has secured the EHR transmission with superior performance.

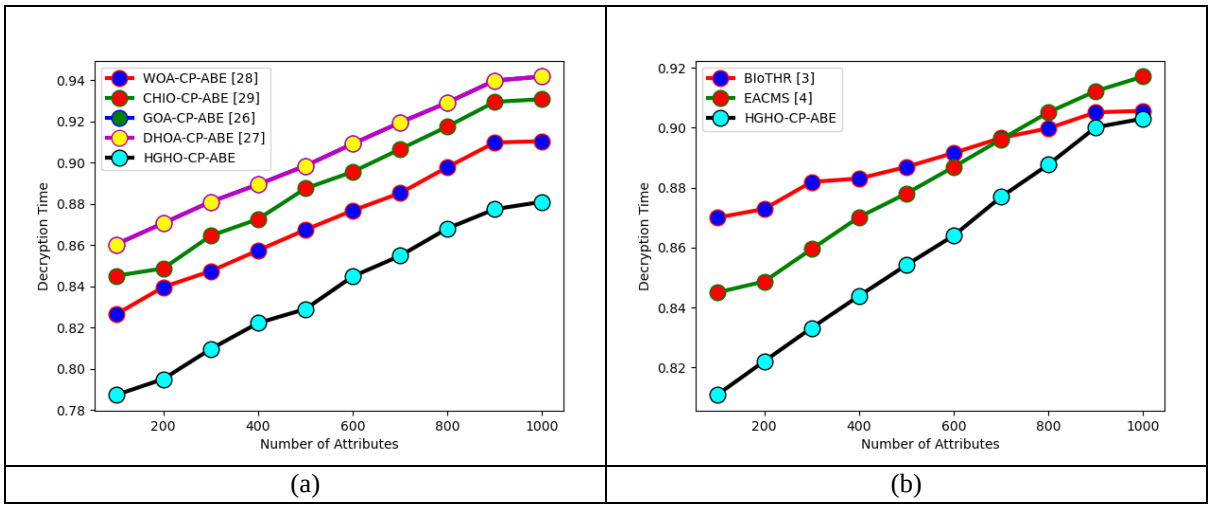


6. Convergence analysis on proposed permissioned blockchain-based secured EHR model.

5.3 Decryption time analysis

The proposed model based on the heuristic-based CP-ABE approach is analyzed to show efficient decryption performance and time efficiency, as shown in Fig. 5. Here, the analyses are done between the algorithms and other baseline approaches. The developed method reveals a minimum decryption time for retrieving the medical records, where the proposed model is 11.67% and 13.6% superior to BIoTHR and EACMS, respectively.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 2102-2120
https://publishoa.com
ISSN: 1309-3452

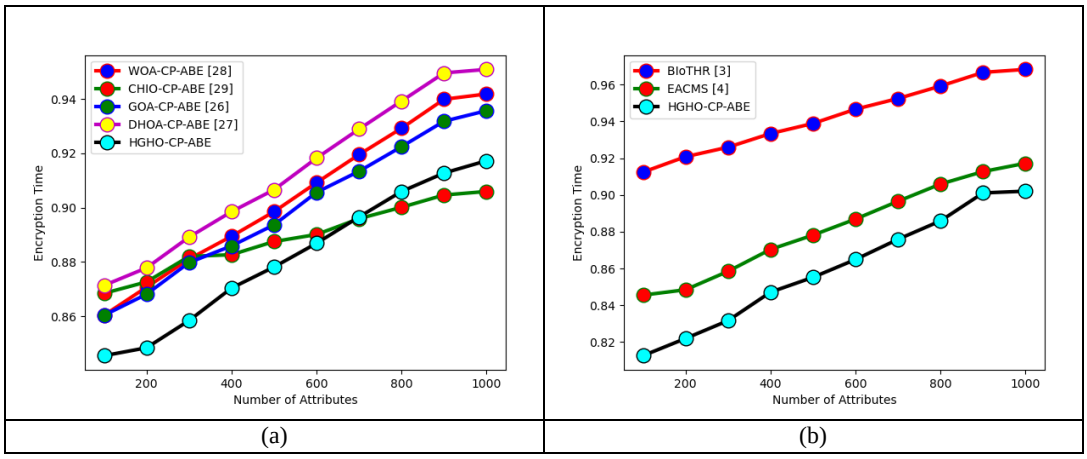


(a) (b)

6. Decryption time analysis on proposed permissioned blockchain-based secured EHR model with "(a) different heuristic algorithms and (b) existing models."

5.4 Encryption time analysis

The evaluation was made between the proposed and conventional algorithms to check the encryption time of the medical records, as in Fig. 6. The proposed HGHO-CP-ABE shows 12.6% and 13.2% improved than BIoTHR and EACMS, demonstrating that less encryption time is required for the proposed model.



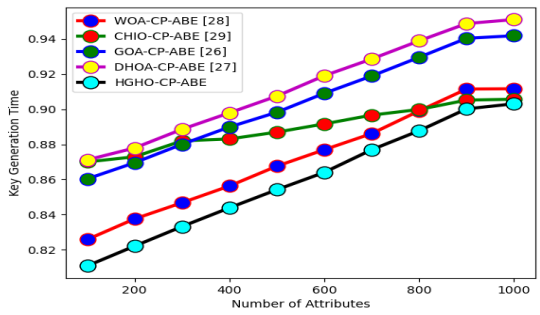
(a) (b)

6 Encryption time analysis on proposed permissioned blockchain-based secured EHR model with "(a) different heuristic algorithms and (b) existing models."

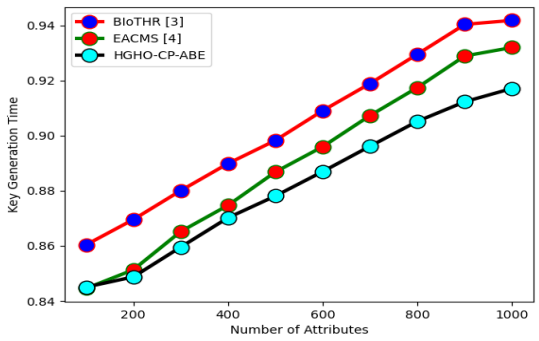
JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 2102-2120
https://publishoa.com
ISSN: 1309-3452

5.5 Key generation time analysis

The key generation in the proposed HGHO-CP-ABE-based data encryption approach was tested with different algorithms and existing models, as in Fig. 7, at a different number of attributes. The proposed model has secured medical records in the EHR system with high security by performing less time for key generation, which is observed to be 14.5%, 16.7%, 12.3%, and 11.5% enhanced WOA-CP-ABE, CHIO-CP-ABE, GOA-CP-ABE, and DHOA-CP-ABE.



(a)



(b)

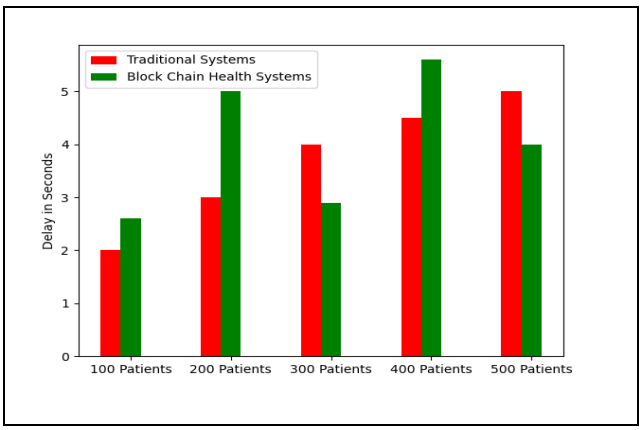
9. Key generation time analysis on proposed permissioned blockchain-based secured EHR

10. model with "(a) different heuristic algorithms and (b) existing models."

5.6 Transactional latency analysis

The transactional latency was evaluated for developed blockchain-based and conventional systems by increasing the patient count in Fig. 6. The blockchain-based systems confirm significantly less delay at 500 patients and thus, show the effective data transaction in the HR systems

.

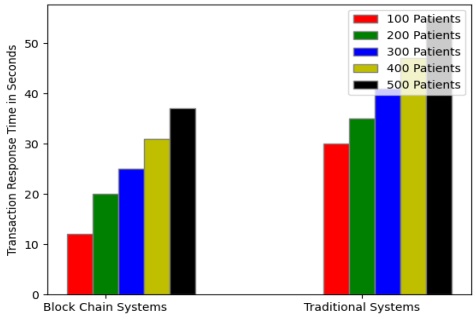


11. Transactional latency analysis on proposed permissioned blockchain-based secured EHR model.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 2102-2120
https://publishoa.com
ISSN: 1309-3452

5.7 Transactional time analysis

The evaluation is made to verify the adequate transactional time in the proposed permissioned blockchain-based EHR security model, as shown in Fig. 9. This analysis confirms that the transactional time of the blockchain-based systems are seems to be less when compared with the traditional systems .



12. Transactional time analysis on proposed permissioned blockchain-based secured EHR model.

7. Conclusion

This paper has developed a new permissioned blockchain-based EHR security model with the optimization approach for securing the EHR of the patients in the hospital. Here, the developed HGHO was used for selecting the optimal keys required for the data encryption. The HGHO-based CP-ABE model has secured less computational time, encryption time, and ciphertext size. The evaluation has shown that the proposed HGHO- CP-ABE approach has given 12.4% and 14.5% improved encryption performance to BIoTHR and EACMS. Thus, the enhanced security performance of the proposed permissioned blockchain-based EHR security model was observed more than the conventional techniques.

Refrences

[1]. Y. Zhuang, L. R. Sheets, Y. -W. Chen, Z. -Y. Shae, J. J. P. Tsai and C. -R. Shyu, "A Patient-Centric Health Information Exchange Framework Using Blockchain Technology," IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 8, pp. 2169-2176, Aug. 2020.

[2]. S. Niu, L. Chen, J. Wang and F. Yu, "Electronic Health Record Sharing Scheme With Searchable Attribute-Based Encryption on Blockchain," IEEE Access, vol. 8, pp. 7195-7204, 2020.

[3]. P. P. Ray, B. Chowhan, N. Kumar and A. Almogren, "BIoTHR: Electronic Health Record Servicing Scheme in IoT-Blockchain Ecosystem," IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10857-10872, 1 July1, 2021.

[4]. A. R. Rajput, Q. Li, M. Taleby Ahvanooey and I. Masood, "EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain," IEEE Access, vol. 7, pp. 84304-84317, 2019.

[5]. L. Tan, K. Yu, N. Shi, C. Yang, W. Wei and H. Lu, "Towards Secure and Privacy-Preserving Data Sharing for COVID-19 Medical Records: A Blockchain-

Empowered Approach," IEEE Transactions on Network Science and Engineering, vol. 9, no. 1, pp. 271-281, 1 Jan.-Feb. 2022.

[6]. Usharani Chelladurai & Seethalakshmi Pandian "A novel blockchain-based electronic health record automation system for healthcare," Journal of Ambient Intelligence and Humanized Computing, vol. 13, pp. 693–703, 2022.

[7]. Gayathri Nagasubramanian, Rakesh Kumar Sakthivel, Rizwan Patan, Amir H. Gandomi, Muthuramalingam Sankayya & Balamurugan Balusamy "Securing e-health records using keyless signature infrastructure blockchain technology in the cloud," Neural Computing and Applications, vol. 32, pp. 639–647, 2020.

[8]. A. Roehrs, C. A. da Costa, R. da Rosa Righi, S. J. Rigo and M. H. Wichman, "Toward a Model for Personal Health Record Interoperability," IEEE Journal of Biomedical and Health Informatics, vol. 23, no. 2, pp. 867-873, March 2019.

[9]. G. Tsang, S. -M. Zhou and X. Xie, "Modeling Large Sparse Data for Feature Selection: Hospital Admission Predictions of the Dementia Patients Using Primary Care Electronic Health Records," IEEE Journal of Translational Engineering in Health and Medicine, vol. 9, pp. 1-13, 2021.

[10]. B. Shickel, P. J. Tighe, A. Bihorac and P. Rashidi, "Deep EHR: A Survey of Recent Advances in Deep Learning Techniques for Electronic Health Record (EHR) Analysis," IEEE Journal of Biomedical and Health Informatics, vol. 22, no. 5, pp. 1589-1604, Sept. 2018.

[11]. J. Zhang, K. Kowsari, J. H. Harrison, J. M. Lobo and L. E. Barnes, "Patient2Vec: A Personalized Interpretable Deep Representation of the Longitudinal Electronic Health Record," IEEE Access, vol. 6, pp. 65333-65346, 2018.

[12]. H. Duan, Z. Sun, W. Dong, K. He and Z. Huang, "On Clinical Event Prediction in Patient Treatment Trajectory Using Longitudinal Electronic Health Records," IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 7, pp. 2053-2063, July 2020.

[13]. M. E. Hossain, A. Khan, M. A. Moni and S. Uddin, "Use of Electronic Health Data for Disease Prediction: A Comprehensive Literature Review," IEEE/ACM Transactions on Computational Biology and Bioinformatics, vol. 18, no. 2, pp. 745-758, 1 March-April 2021.

[14]. A. Shahnaz, U. Qamar and A. Khalid, "Using Blockchain for Electronic Health Records," IEEE Access, vol. 7, pp. 147782-147795, 2019.

[15]. A. Dalley, J. Fulcher, D. Bomba, K. Lynch and P. Feltham, "A technological model to define access to electronic clinical records," IEEE Transactions on Information Technology in Biomedicine, vol. 9, no. 2, pp. 289-290, June 2005.

[16]. G. Harerimana, J. W. Kim, H. Yoo and B. Jang, "Deep Learning for Electronic Health Records Analytics," IEEE Access, vol. 7, pp. 101245-101259, 2019.

[17]. X. Liu, Z. Wang, C. Jin, F. Li and G. Li, "A Blockchain-Based Medical Data Sharing and Protection Scheme," IEEE Access, vol. 7, pp. 118943-118953, 2019.

[18]. T. F. Stafford and H. Treiblmaier, "Characteristics of a Blockchain Ecosystem for Secure and Sharable Electronic Medical Records," IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1340-1362, Nov. 2020.

[19]. S. M. Shah and R. A. Khan, "Secondary Use of Electronic Health Record:

Opportunities and Challenges," IEEE Access, vol. 8, pp. 136947-136965, 2020.

[20]. Mohammad Moussa Madine, Ammar Ayman Battah, Ibrar Yaqoob, Khaled Salah, Raja Jayaraman, Yousof, "Blockchain for Giving Patients Control Over Their Medical Records," IEEE Access, vol. 8, pp. 193102-193115, 2020.

[21]. [21] X. Liu, Z. Wang, C. Jin, F. Li and G. Li, "A Blockchain-Based Medical Data Sharing and Protection Scheme," IEEE Access, vol. 7, pp. 118943-118953, 2019.

[22]. Hemant B. Mahajan, Ameer Sardar Rashid, Aparna A. Junnarkar, Nilesh Uke, Sarita D. Deshpande, Pravin R. Futane, Ahmed Alkhayyat & Bilal Alhayani "Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems," Applied Nanoscience, 2022.

[23]. Priti Tagde, Sandeep Tagde, Tanima Bhattacharya, Pooja Tagde, Hitesh Chopra, Rokeya Akter, Deepak Kaushik & Md. Habibur Rahman "Blockchain and artificial intelligence technology in e-Health," Environmental Science and Pollution Research, vol. 28, pp. 52810–52831, 2021.

[24]. Arvind Panwar & Vishal Bhatnagar "A cognitive approach for blockchain-based cryptographic curve hash signature (BC-CCHS) technique to secure healthcare data in Data Lake," Soft Computing, 2021.

[25]. Azath Mubarakali "Healthcare Services Monitoring in Cloud Using Secure and Robust Healthcare-Based BLOCKCHAIN (SRHB)Approach," Mobile Networks and Applications, vol. 25, pp. 1330–1337, 2020.

[26]. Shahrzad Saremi, Seyedali Mirjalili and Andrew Lewis, "Grasshopper Optimisation Algorithm: Theory and application", Advances in Engineering Software, vol. 105, pp. 30–47, 2017.

[27]. G Brammya, S Praveena, N S Ninu Preetha, R Ramya, B R Rajakumar, and D Binu, "Deer Hunting Optimization Algorithm: A New Nature-Inspired Meta-heuristic Paradigm", 24 May 2019.

[28]. Q. Zhang and L. Liu, "Whale Optimization Algorithm Based on Lamarckian Learning for Global Optimization Problems," IEEE Access, vol. 7, pp. 36642-36666, 2019.

[29]. S. Amini, S. Ghasemi, H. Golpira and A. Anvari-Moghaddam, "Coronavirus Herd Immunity Optimizer (CHIO) for Transmission Expansion Planning," IEEE International Conference on Environment and Electrical Engineering and IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe), 2021.