Complex & Intelligent Systems (2022) 8:625–640
https://doi.org/10.1007/s40747-021-00549-w

ORIGINAL ARTICLE

Hyperledger blockchain enabled secure medical record management with deep learning-based diagnosis model

Naresh Sammeta[1,2] · **Latha Parthiban**[3]

Received: 27 May 2021 / Accepted: 17 September 2021 / Published online: 9 October 2021

Abstract

In recent times, advanced developments in healthcare sector result in the generation of massive amounts of electronic health records (EHRs). EHR system enables the data owner to control his/her data and share it with designated people. The vast volume of data in the healthcare system makes it difficult for data to ensure security and diagnostic processes. To resolve these issues, this paper develops a new hyperledger blockchain enabled secure medical data management with deep learning (DL)-based diagnosis (HBESDM-DLD) model. The presented model involves distinct stages of operations such as encryption, optimal key generation, hyperledger blockchain-based secure data management, and diagnosis. The presented model allows the user to control access to data, permit the hospital authorities to read/write data, and alert emergency contacts. For encryption, SIMON block cipher technique is applied. At the same time, to improve the efficiency of the SIMON technique, a group teaching optimization algorithm (GTOA) is applied for the optimal key generation of the SIMON technique. Moreover, the sharing of medical data takes place using multi-channel hyperledger blockchain that utilizes a blockchain for storing patient visit data and for the medical institutions to record links for the EHRs saved in external databases. Once the data are decrypted at the receiving end, finally, variational autoencoder (VAE)-based diagnostic model is applied to detect the existence of the diseases. The performance validation of the HBESDM-DLD model takes place on benchmark medical dataset and the results are inspected under various performance measures. The experimental results proves that the HBESDM-DLD methodology is superior to state-of-the-art methods.

Keywords Blockchain · Electronic health records · SIMON · Variational autoencoder · Deep learning

Introduction

The personal health record (PHR) system is a significant resolution in healthcare sector to properly manage the patient details. The PHR scheme allows interchanging of data with healthcare providers and assists to predict health problems. It stores the health relevant information and contains highly sensitive data [1]. Few improper alterations/modifications of some PHR information might result in serious consequences. Therefore, secrecy turns to be the major factor for PHR systems. A tamper-resistant feature is a vital component for the PHR system. It considerably gives the higher quality protective personal healthcare when the lifetime health relevant data of a person could be highly stored and captured on tamper-resistant storage. Blockchain's cryptographic verifiability, backup, and immutability properties could make it an effective tamper-resistant storage solution for the PHR system.

Data sharing is the essential stage to attain highest benefits from an innovative study. However, it is critical to recognize the 3 Ws, such as where, what, and when. These queries should be accurate before starting the process of data sharing. There are few scopes to operate and the data set owner needs to provide reward/incentives. This study gives secured sharing of data with leverage benefits of blockchain [2]. Blockchain, a shared ledger is a novel tendency in the IT field. The consensus method is assumed as a significant and funda-

✉ Naresh Sammeta
samnaresh@gmail.com

Latha Parthiban
lathaparthiban@yahoo.com

1 JNTUK, Kakinada, Andhra Pradesh 533003, India

2 Department of Computer Science and Engineering, R.M.K. College of Engineering and Technology, Chennai, Tamilnadu 601206, India

3 Department of Computer Science, Pondicherry University Community College, Puducherry 605008, India

mental creation as stated by an expert of Silicon Valley. An essential characteristic of blockchain is trust that is attained by removing unauthorized parties. At present, blockchain is utilized in various fields, such as health care, IoT, cloud, information security data trading, etc. [3]. The main challenges in this data sharing are related to the misinterpretation and misuse of information.

The cloud server, in general, is a central authority that holds a huge amount of data. Decentralized storage is a system that allows data to be stored as a shared ledger on several network nodes. The challenge is processing and storage restriction of network nodes. Data accessibility is guaranteed with a storage on decentralized framework and IPFS. In presented architecture, the data owners do not have whole access to information. Mostly, the owner itself is not included in data sharing [4–6]. For instance, the owner is passive entity, when escrow is individually accountable for payment settlements and data distribution. Without blockchain, it is highly complex to ensure the fund transparencies in which the reasonable money sharing could not be assured. In this condition, blockchain could provide transparency and trust between the network nodes for reasonable sharing of obtained payment from the data requestor. Alternatively, integrity and quality of information could not have cooperated if a client is paying to acquire the content. For addressing these problems, an individual resolution is presented. In this condition, owner (i.e., patient) itself handles the health record distribution by removing third parties. The data owner could fix accessing guidelines, and thus, information is not revealed to third parties. In federated learning (FL), organizations pool data to construct a unified, sophisticated machine learning model that functions as a closed-loop system [7, 8]. In the near future, the ability to have rich customer insights will enable businesses to achieve incredible outcomes such as improving consumer data privacy, data security, data-access rights, and access to heterogeneous data. FL makes it possible for machine learning algorithms to have practical experience using a wide range of diverse datasets, all of which are located at various places. This technique facilitates the creation of models that various companies may work on together, but without the need to exchange sensitive data. The main contributions of this article includes the following.

- The presented model develops a new hyperledger blockchain enabled secure medical data management with deep learning (DL)-based diagnosis (HBESDM-DLD) model.
- It allows the user to control access to data, permit the hospital authorities to read/write data, and alert emergency contracts.
- The proposed HBESDM-DLD model makes use of SIMON block cipher technique to encrypt the health records.
- The effectiveness of the SIMON technique can be enhanced using group teaching optimization algorithm (GTOA) with the optimal key generation process.
- Furthermore, medical record sharing process is performed via multi-channel hyperledger blockchain.
- The proposed model integrates the federated learning (FL) concept along with the blockchain technology. Next to the data decryption process, variational autoencoder (VAE)-based diagnostic model is employed for effective disease diagnosis.
- The HBESDM-DLD model's experimental results are analyzed by numerous performance measures using benchmark medical datasets.

Related works

This section reviews the recent state-of-art blockchain enabled healthcare systems, particularly developed for secure medical data transmission. Nguyen et al. [9] proposed a new hybrid approach of data sharing and offloading for healthcare via blockchain and edge cloud. Initially, an effective data offloading system is presented, while IoT healthcare data are offloaded to an adjacent edge server for processing data with privacy attentiveness. Next, a data sharing system is combined with data interchange between healthcare clients using blockchain. Specifically, a reliable access control technique is introduced by an intelligent contract management for accessing authentication to accomplish secured EHR distribution. Al Mamun et al. [10] presented a blockchain integrated with IPFS solution architecture for EMR in the healthcare field. It aims at designing blockchain for EMR and gives access rules to several clients. The presented architecture protects person secrecy, and enables suitable access by the permitted authority like healthcare suppliers to medical data. Bisogni et al. [11] proposed a new encryption system particularly for authorizing and signing transactions in digital/intelligent contract system. The facial recognition is utilized as biometric key, encoded by CNN and FaceNet. Yates [12] proposed a new hybrid method of data sharing and offloading for healthcare via edge cloud and blockchain. Initially, an effective data offloading system is projected when IoT healthcare data are offloaded in adjacent edge server for processing data with privacy attentiveness. Next, a data sharing system is combined for enabling data interchange between healthcare centers using blockchain. Mainly, a reliable access control system is introduced by an intelligent contract management for accessing authentication to attain secured EHR distribution. Huang and Lee [13] incorporated the strength of blockchain and CC to create privacy protection system for medical data using blockchain and CC. This system presents CC and provides a service for blockchain nodes with CC server where it gathers, exam-

ines, processes, and preserves medical data in the identity authentication interface and resolves inadequate calculating capabilities of few nodes in blockchain for verifying consistency and authenticity. Hylock and Zeng [14] introduced HealthChain, a new patient cantered blockchain architecture. The aim is to boost person appointment, regulated dissemination, and data curation of collected data in an interoperable, secured platform. Additionally, person can obtain a cryptographic identification as private and public key pairs. The public keys are kept in the blockchain and appropriate to secure and verify transactions. Additionally, the envisaged scheme utilizes proxy re-encryption (PRE) for sharing data via intelligent contract, revocable that ensures the maintenance of confidentiality and privacy. Sun et al. [15], presented a distributed electronic medical record searchable system using leveraging blockchain and intelligent contract technique. Initially, they execute hash calculations on electronic medical data and store equivalent value on blockchain for ensuring its authenticity and integrity. After, they encrypt it in the IPFS, the distributed storage protocol. This operation could resolve central data storage of the server of various medical organizations; however, it is optimum in reducing the stress from data storage and higher frequency accessing to blockchain. Following, the encrypted keyword index data are stored on the Ethereum blockchain, along with a smart contract that is used to comprehend the keyword search rather than a central third party. Also, they utilized attribute-based encryption system for ensuring that attributes can meet the access policy for decrypting the encrypted data. Chen et al. [16] implemented a storage system for managing personal medical data based on blockchain and cloud storage. In addition, a medical record sharing service architecture is illustrated. The presented storage and sharing systems do not depend on third party and none of the parties have an authority for affecting the process. A new EHR management system called PREHEALTH, using distributed ledger technology and an Identity Mixer, has been proposed (Idemix). A proof-of-concept implementation using permissioned blockchain architecture to simulate how applications may communicate with permissioned blockchains. It is possible to create a record keeping system while maintaining patient confidentiality and unlikability. Experimental results show that the system is practical for mass-market use. Ekblaw et al. [17] implemented MedRec leverages blockchain features to guarantee secure authentication, confidentiality, and accountability in addition to data sharing. Weaved into the services providers' existing local data storage solutions, the system's modular architecture integrates, allowing interoperability and making the system flexible and useful.

To motivate academics, public health authorities, and others to join in the network as blockchain "miners," we provide rewards in the form of cryptocurrency. With this in place, miners are able to obtain anonymised data rewards, and at the same time contribute to and maintain the network via Proof of Work. As MedRec empowers data economics, it supplies large data to researchers and engages patients and clinicians in determining whether to make information publicly available. The summary of proposed solutions is impacted by hyperledger blockchain, as shown in Table 1.

Literature survey

Vora et al. [18] in this study suggest a blockchain-based system for storing and managing EHRs that are efficiently. This further helps to ensure the patient privacy while also providing a secure and efficient method of accessing medical data for providers, patients, and third parties. Our study seeks to measure the framework's capacity to meet the demands of patients, healthcare providers, and third parties, and it also aims to understand how the framework retains privacy and security while accommodating the emerging healthcare 4.0. This is important, since it solves the escrow problem, as well as the manner of distributed data storage on the blockchain [19]. The protocol avoids collusion attack by distributing the pseudorandom function seeds across authorities, ensuring that no more than $N - 1$ of the authorities are corrupt. This signature method is formally proven to be safe when applying the computational bilinear Diffie–Hellman assumption. This article offers a hybrid architecture that utilizes both blockchain and edge nodes to provide access control of EHR data [20]. The identity and access control restrictions are enforced using a blockchain-based controller that is also a tamper-proof log of access occurrences. The second is that off-chain edge nodes store the EHR data and use ALFA, a predefined set of attributes, to provide attribute-based access control on EHR data in cooperation with the blockchain-based access control logs. Sharma et al. [21] are currently developing a system that implements electronic health records (EHRs) using blockchain technology, with the aim of making them safer and more private. This technology will use cryptography and decentralization to regulate access to information. Also, it keeps the balance between privacy and accessibility with regard to data. Our project's major aim is to present electronic healthcare's data privacy and security problems in a new light. Using hyperledger fabric, we implement a distributed system made out of existing EHRs that utilize consortium blockchain [22]. The same ledger on which the address of a patient record in an EHR is written is used by peers to keep the blockchain that contains all patient records [23]. Every patient has their own individual certificate, which is issued by a local certificate authority that partners with other certificate authorities to form a channel of the network. When patients' data are transmitted, we utilize a proxy re-encryption technique that safeguards their privacy. The Federated Learning setup applies machine learning

Table 1 Summary of proposed solutions related to blockchain technology

Author	Health data or information systems	Future systems to be improved/addressed	Methodology or challenges addressed in article
Tian, He and Ding	Personal health records	Limited algorithmic notations with discussion of results for simulated security analysis and performance evaluation	Performance evaluation and security analysis
W Wang	Automated diagnostic service for patients	Collection of information about symptoms of dyslexia and the purpose of diagnostics, decision-support, and research process	Access control, data integrity, interoperability
K. Fans	Electronic health records	Sharing of healthcare information for research and clinical usage	Access control, identity management, and authentications
J. Chen	Electronic health records	Collection of patients information, archiving, and healthcare data sharing for clinical purposes	Data integrity, access control, authentications
H. Li	Electronic health records	Storing of health information	Privacy, data integrity, and authentications process
X. Zhang	Electronic health records	Retrieval information from EHR	Data integrity and access control systems
Y. Sun	Electronic health records	Healthcare data sharing between hospital or clinical institutions	Data provenance, access authentications systems
P. Zhang	Electronic health records	Healthcare data sharing between hospital for research	Access control

with clients like mobile devices or large companies training a model together on the back of a centralized service provider [24]. The data are decentralized and retained by the participants in the learning process. FL is focused on collecting the right data while minimizing the many privacy concerns and costs associated with the usage of standard centralized machine learning and data science methods. The article focuses on recent breakthroughs and provides a wide collection of open issues and challenges, all motivated by the tremendous increase in FL research. Wang et al. [25] used design and implementation of a unique privacy-preserving inference information flow to show it through the design and implementation of a novel privacy-preserving inference information flow. Splitting the model up farther along the computing chain has a large effect on the computation time of inference and the payload size of activation signals. This leads to more model secrecy at the cost of greater computation time. Rajadurai et al. [26] apply a method to determine the latency of a static schedule for a given unfolding factor on a heterogeneous multiprocessor platform, while simultaneously maintaining an optimal throughput for an SDF graph. The system model comprises a synchronous data flow graph and an execution platform, all of which is made up of timed automata. The UPPAAL model checker is used to define the final output.

The proposed HBESDM-DLD model

The presented model in Fig. 1 shows the working process of HBESDM-DLD model which involves distinct stages of operations such as encryption, optimal key generation, hyperledger blockchain-based secure data management, and diagnosis. At the initial stage, the health records owned by the patient are encrypted using SIMON block cipher technique with GTOA-based optimal key generation technique. Next to the data encryption process, the hyperledger blockchain is involved that has a global blockchain and numerous local blockchain for medical institutions. The patient permits access or revokes access to any physician or medical organization. Followed by the legal user can decrypt the cipher data and retrieve the actual health records. At the final stage, the VAE-based diagnostic process is performed to determine the existence of the diseases.

Data encryption process

Generally, light weight cryptographic methods are represented by hash capacities, block ciphers, verified decryption, and encryption modeling procedure. In this research, block ciphers are employed for secure healthcare record management. The evolution of lightweight ciphers starts with an improved advanced encryption standard (AES). At

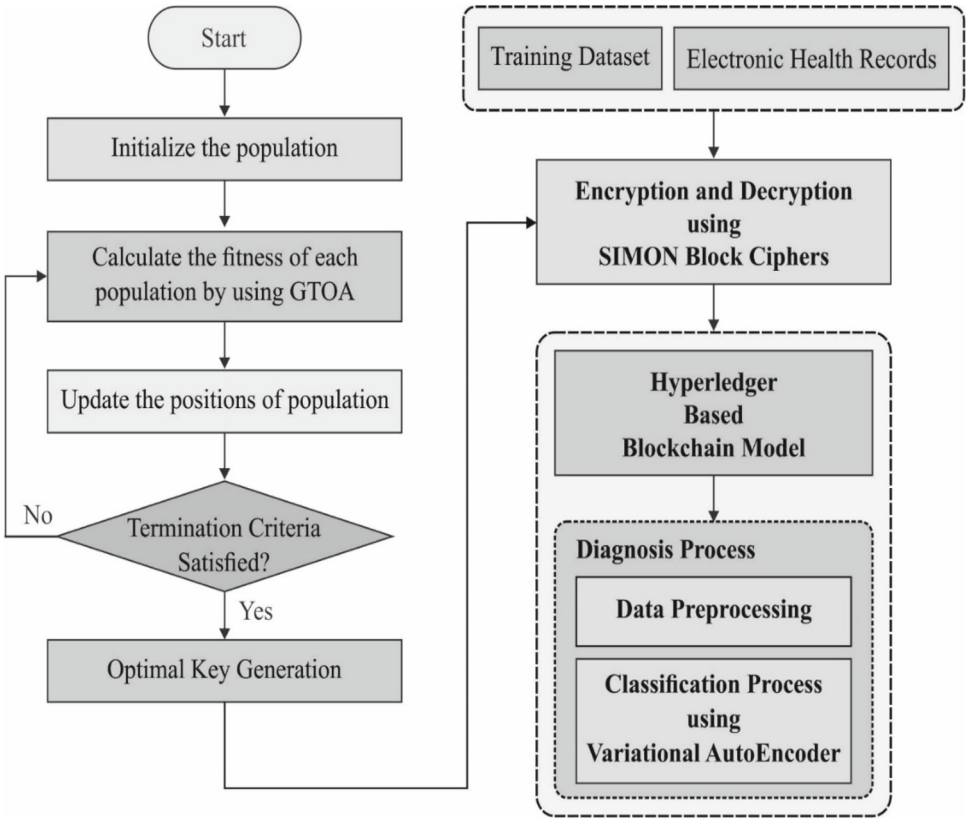


Fig. 1 Block diagram of HBESDM-DLD model

present, several ciphers are available such as, RECTANGLE, SIMON, TWINE, KATAN, SPECK and KLEIN, and SIMON ciphers. SIMON, a lightweight block cipher, is performed based on hash function and efficiency while linked to hardware. This cipher family includes ten functions where two variables differ in structure, especially key size and block. For every block, the key gets varied based on image pixels. Figure 2 illustrates the structure of SIMON block cipher. The block measures the variation from 32 to 128 bits, comprising the approximation of 16. It executes an act on fixed size block of plain text and carries block of cipher content [27]. The SIMON cipher contains nonlinear and direct features for security study with the block size and data. While using a set of input variances, the individual could consider a tree for each difference in all rounds, generating some of the possible output variances.

Assume that the essential features are extended to further rounds on off-chance, and individuals could utilize solid structure of round capability. The SIMON key calendar uses the round reliability for the features of key schedules and develops quantity of pixel esteem in an image. There is one single key difference indication for the 15-round SIMON48 on the lightweight block cipher. The quality of this block cipher is not designed to be ideal. The selected optimizer produces the best solution where the quality in this approach is guaranteed to have least number of active S-boxes.

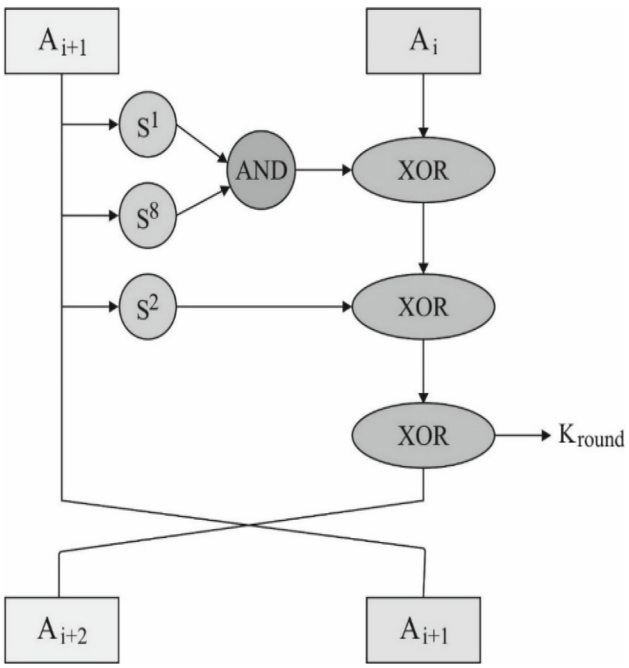


Fig. 2 Structure of SIMON block cipher

Currently, while performing the cipher module for secure data transmission, some major components are included namely encryption, round, bit, and decryption. One example of the SIMON cipher round function is illustrated in Fig. 3, which depicts the process of splitting an input plaintext block ($2n$) into two equal-sized words (each one is n-bit). Three shifts to the left and bitwise AND logic operations are done on the left half block in each round function. The right half block is XORed with the XOR result, and the key used is the round one, as shown in Fig. 2. The produced value is then written back to the left block, while the left half value is moved to the right block at the conclusion of each round. As long as the total number of rounds for the implemented configuration remains the same, this round procedure is continually repeated. F can be represented by Eq. (1). The SIMON cipher with $2n$-bit blocks are equated as follows:

$$\text{EncDI} = \text{Cipher}^{i}_{q_l}, \ldots \text{Cipher}^{n}_{q_1}, i > 1. \tag{1}$$

This Cipher $C^{i}_{q_l} \leq i \leq q$ is named as round functions with round keys. This function is analogous and is known as an iterated block cipher. For encryption, the SIMON round capability is given by

$$RF\left(w_l, w_r, k_{\text{round}}\right) = \left(\left(S^1\left(w_l\right) \& S^8\left(w_l\right)\right) \oplus S^2\left(w_l\right) \oplus w_r \oplus k_{\text{round}}, w_l\right). \tag{2}$$

The inverse function is utilized for decrypting the data, as shown in Eq. (3)

$$RF^{-1}\left(w_l, w_r, k\right) = \left(w_r, \left(S^1\left(w_l\right) \& S^8\left(w_l\right)\right) \oplus S^2\left(w_r\right) \oplus w_l \oplus k_{\text{round}}\right). \tag{3}$$

The term described in Eq. (3) is, w_l represents left most word of a provided block, w_r indicates right most word, and k_{round} represents proper round key.

HBESDM-DLD algorithm

Algorithm 1 HBESDM-DLD secure medical record management.

Algorithm 1. HBESDM-DLD secure medical data management and SIMON block cipher addition

Input: Reading EHR for a patient P1

Output: Patient P1 HBESDM-DLD and add blocks to Patient P1 blockchain

Step 1: EHR ← Patient P1 and read EHR

Step 2: Public Key and Private Key ← key generation using SIMON block cipher

Step 3: For encryption patient p1 ← Public key

Step 4: Doctor ← shared private key and Insurance Agency for Decryption purpose

Step 4: Encrypted EHR ← Encrypt EHR Public key-based SIMON

Step 5: SIMON ← Hash key for EHR encryption based on GTOA

Step 6: VAE ← Generate disease diagnosis process for encrypted Patient P1 with HER

Step 7: Create a hyperledger block for Patient P1 blockchain using the patient user id, password, and patient code

Step 8: Block ← Put hash key value, encrypted EHR with VAE

Step 9: HBESDM-DLD-based secure block to Patient P1 blockchain

Step 10: Stop

Optimal key generation process

From the master key, SIMON cipher gives key expansion by generating whole round keys. The chosen $SIMON64/128$ formation creates 32-bit-sized round keys from the early 128-bit master key. It ensures the round by combining the saved previous round keys (key word variable) with reliable and 1 bit round. The key expansion task utilizes associated activities.

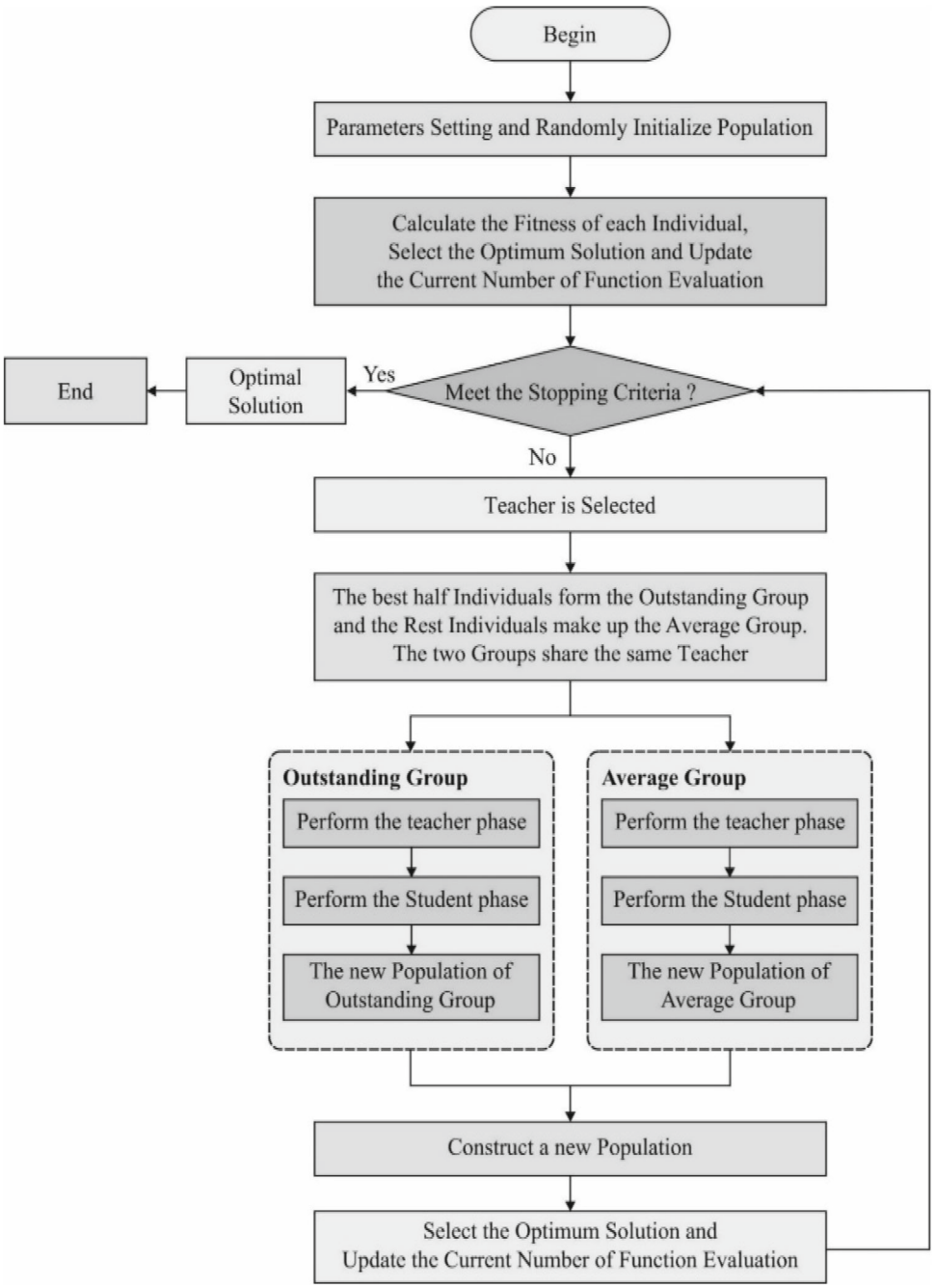
- Bitwise XOR, denotes $a \oplus b$.
- Left circular shift, F^j, by j bits and right circular shift, F^{-j}, by j bits
- Round counter, where $0 \leq i \leq T-1$ and constant sequence, where $j = 0, 1, 2, 3, 4$
- Round key (sub-key), number of cipher rounds and constants.
- Right bitwise rotation ROR, destined by $s^{-c}(a)$, while c represents number of rotations.

The operation of key expansion is given in Eq. (4)

$$\text{Key}_i\left(k, c, z_j\right) = F\left(k_{i+3}, k_{i+1}\right) \oplus S^{-1}\left(F\left(k_{i+3}, k_{i+1}\right)\right) \oplus k_i \oplus c \oplus \left(z_j\right)_i. \tag{4}$$

Among the several generated keys, an optimal key can be selected to decrypt the data. For selecting the optimal key, the GTOA is applied to optimize the value as minimum or maximum. The presented GTOA is stimulated by a group teaching technique. The aim is to enhance the knowledge of

Fig. 3 Flowchart of GTOA



the entire class. Consider several variances between students and it is complex to be executed in real time. To adjust this method to be appropriate for optimization method, they initially consider population, decision parameter, and fitness value corresponding to the students [28]. Later, a simple group teaching module with no loss of generalization is created. Using pseudorandom sortition and transaction witness, the technique achieves consensus. To increase the algorithm's scalability, three dimensions of throughput, latency, and latency have been added to the formula. A consensus method that is good in terms of scalability, low latency, high throughput, and decentralization should be implemented. This study proposes an improved hybrid consensus algorithm that uses the GTOA algorithm. Verifiable cryptographic sortition dynamically picks the consensus node, allowing many nodes to participate in the consensus fairly while ensuring low latency and high throughput. There are four stages in the presented module, namely, capability grouping, teacher allocation, student stage, and teacher stage. The four stages are defined as follows.

Capability grouping stage

With no loss of generalization, the knowledge of entire classes is considered a normal distribution. It is given by

$$f(x) = \frac{1}{\sqrt{2\pi}\,\delta} e^{\frac{(x-u)^2}{2\delta^2}}, \tag{5}$$

where x represents value of normal distribution function, u denotes mean knowledge of entire classes, and δ indicates standard deviation (SD). The worthy teacher is assumed to enhance the mean knowledge u; however, it decreases the SD δ. To attain this objective, the teacher must create an appropriate teaching strategy for their students. To illustrate the group teaching feature, with no loss of generalization, every student is separated into two smaller groups based on the capability of adapting knowledge in GTOA. It is emphasized that the SD of outstanding and average groups might be greater than transfer of teaching events. To tackle this problem, capability grouping is an energetic procedure in GTOA that is executed over a learning cycle. Figure 3 demonstrates the flowchart of GTOA.

Teacher stage

It implies that individual student gains knowledge from their teacher that relates to the determined subsequent rule. The teacher creates various teaching strategies for average and outstanding groups in the presented GTOA.

Teacher stage I

Insight of stronger capability of adapting knowledge, the teacher pays more attention to enhance knowledge of outstanding group. Particularly, the teacher could attempt their maximum to enhance the mean knowledge of entire classes. Furthermore, differences in applying knowledge among students must be anticipated. Therefore, the student of outstanding group could attain their knowledge as

$$x^{t+1}_{\text{teacher},i} = x^t_i + a \times \left(T^t - F \times \left(b \times M^t + c \times x^t_i\right)\right) \tag{6}$$

$$M^t = \frac{1}{N}\sum_{i=1}^{N} x^t_i \tag{7}$$

$$b + c = 1, \tag{8}$$

where t represents present number of iterations, N indicates number of students, x^t_i denotes knowledge of student i at time t, T^t indicates knowledge of teacher at time t, M^t represents mean knowledge of such group at time t, F indicates teaching factor, $x^{t+1}_{\text{teacher},i}$ represents knowledge of student i at time t via learning from their teacher, and a, b, and c denote arbitrary value between zero and one. The value of F is either one or two as made.

Teacher stage II

Consider the least capability of adapting knowledge, a teacher focuses on average group compared to outstanding group by following rules that inclines to enhance the students' knowledge from the perception of persons. Therefore, the student of average group could attain their knowledge as

$$x^{t+1}_{\text{teacher},i} = x^t_i + 2 \times d \times \left(T^t - x^t_i\right), \tag{9}$$

where d represents arbitrary value between zero and one. Additionally, individual student may not attain the knowledge at teacher stage is tackled as (taking the smallest problem as an instance) follows:

$$x^{t+1}_{\text{teacher},i} = \begin{cases} x^{t+1}_{\text{teacher},i}, f\left(x^{t+1}_{\text{teacher},i}\right) < f\left(x^t_i\right) \\ x^t_i, f\left(x^{t+1}_{\text{teacher},i}\right) \geq f\left(x^t_i\right) \end{cases}. \tag{10}$$

Student stage

It includes stages I and II related to the stated third rule. In free time, individual student could attain their knowledge in two distinct manners such as individual by self-teaching and by interacting with other students that are given by

$$x^{t+1}_{\text{student},i} = \begin{cases} x^{t+1}_{\text{teacher},i} + e \times \left(x^{t+1}_{\text{teacher},1} - x^{t+1}_{\text{teacher},j}\right) + g \times \left(x^{t+1}_{\text{teacher},i} - x^t_i\right), f\left(x^{t+1}_{\text{teacher},i}\right) \\ x^{t+1}_{\text{teacher},i} - e \times \left(x^{t+1}_{\text{teacher},i} - x^{t+1}_{\text{teacher},j}\right) + g \times \left(x^{t+1}_{\text{teacher},i} - x^t_i\right), f\left(x^{t+1}_{\text{teacher},i}\right) \end{cases}, \tag{11}$$

where e and g represent two arbitrary amounts in the extent of zero and one, $x^{t+1}_{\text{student},i}$ indicates knowledge of student i at time t via learning from student stage, and $x^{t+1}_{\text{student},j}$ indicates knowledge of student j at time t via learning from teacher. The student $j(j \in \{1, 2, \ldots, i-1, i+1, \ldots, N\})$, he or she is arbitrarily chosen. In Eq. (11), the next item and the third item on the right imply learning from another student and self-teaching, respectively.

Furthermore, individual student may not attain knowledge via student stage is tackled as (taking the least problem as an instance) follows:

$$x^{t+1}_i = \begin{cases} x^{t+1}_{\text{teacher},i}, f\left(x^{t+1}_{\text{teacher},i}\right) < f\left(x^{t+1}_{\text{student},i}\right) \\ \left(x^{t+1}_{\text{student},i}\right), f\left(x^{t+1}_{\text{teacher},i}\right) \geq f\left(x^{t+1}_{\text{student},i}\right) \end{cases}, \tag{12}$$

where x^{t+1}_i represents knowledge of student i at time $t+1$ in learning cycle.

Teacher allocation stage

According to fourth rule, creating a decent teacher allocation technique is essential to enhance the knowledge of students. In GWO, the initial three optimal solutions attained are utilized for guiding hunt of wolves. Stimulated by hunting behavior in GWO, the teacher distribution in presented technique is given by

$$T^t = \begin{cases} x^t_{\text{first}}, & f\left(x^t_{\text{first}}\right) \le f\left(\frac{x^t_{\text{first}}+x^t_{\text{second}}+x^t_{\text{first}}}{3}\right) \\ \frac{x^t_{\text{first}}+x^t_{\text{second}}+x^t_{\text{first}}}{3}, & f\left(x^t_{\text{first}}\right) > f\left(\frac{x^t_{\text{first}}+x^t_{\text{second}}+x^t_{\text{first}}}{3}\right) \end{cases}, \quad (13)$$

where x^t_{first}, x^t_{second}, and x^t_{third} represent first, second, and third optimal students, respectively. To speed up the convergence of the presented GTOA, outstanding and average groups allocate similar teachers.

Hyperledger blockchain

In this study, federated learning process is employed in the blockchain with ML-based disease diagnostic model. Blockchain is a technique that executes shared ledger. It offers availability, suitability, privacy, integrity, and decentralization [29]. The decentralization enables data kept in the Blockchain to be repeated over several computers, avoiding individual point of failure of central server. The availability allows for accessing the data when it is required; nevertheless, few computers fail. Integrity with data maintenance, protecting it from inappropriate modifications. The suitability could trace entire data that have been kept in blockchain. At last, privacy permits the members to remains unidentified. From a technical viewpoint, the blockchain comprises a set of arranged and reliable blocks of chain, which has a header and stores data. The header composed of various features such as signature, identifier, and previous block. The identifier denotes a worldwide unique value with a mathematical function which enclose every block of information. The previous block is in charge of block chaining. For every novel block included in the chain, it would contain the identifier value of previous block, therefore, generating a logical chain of connections. Hyperledger is management that provides various open-source blockchains and hyperledger fabric is one of them. It aims at providing a decentralized environment. It involves endorser peer, order, certificate authority, client, and committing peer. In addition, the components connect utilizing channels that are implemented for enabling the transactions privately and secretly, splitting different domains of application. The fabric certificate authority is responsible for two procedures. Initially, to guarantee various components (user or smart contracts) to use the system that is stated and next, it validates the component and authorizes to use it for certain function (for example carrying out transaction) or access other component resulting to authorization. The committing peer is responsible to persevere the chain sent by the channel generated in the system [30]. Thus, they store various blockchains, for all individuals' channels created. This 'individual chain per channel' technique provides scalability and privacy [31].

On comparing with privacy, the component cannot access a chain from a committed peer interrelated to the channel when the element does not have ease of access to that network. According to scalability, individual for each channel allows the sharing of various transactions and data kept with in various committing nodes, increasing the requested amount where a node gets fulfilled and to increase quantity of data, thus increases the system scalability. Authorizing peers are responsible for two procedures. Initially, it gathers transaction from client, and next, it is analyzed using smart contract system where the transaction has several related rules that should be followed. Gathering peers execute two procedures such as it obtains customer transaction and arrange the transaction in monitoring the blockchain reliability. Consequently, all ordering peers performed on a certain chain must confirm that the transaction is added to the committing peers. It is stated that a person can visit similar medicinal institutions often, and this blockchain saves just single visit. The blockchain for each medicinal institution (so-called local blockchain) stores EHR relevant to the person. To place the blockchain, it is considered that the medicinal institution keeps least structure required to perform the hyperledger network.

In hyperledger Fabric, a smart contract is a chaincode application. A chaincode is usually used to implement network-agreed business logic. Once a chaincode is generated, the resulting state is private to that chaincode and inaccessible by other chaincode. It is possible to call another chaincode if you have the necessary authorization. When thinking about chaincode, it is helpful to consider two different types: chaincode for a system whole chain of application-specific code system chaincode is generally in charge of handling system-related transactions, such as policy configuration and lifecycle management. Users have access to the system chaincode API, though, and are free to customize it for their own purposes. The application chaincode is responsible for keeping application states such as digital assets or arbitrary data entries on the ledger. A chaincode starts with a package that has metadata, such as the name, version, and counterparty signatures, which is used to guarantee the integrity of the code and metadata. After the chaincode package has been loaded on the counterparties' network nodes, the software is automatically installed on the local computers of the parties. To register the participants, a registration function is performed within the smart contracts

(chaincode) for the private health authority authorized by the fabric network administrator to administer and manage the fabric network. The healthcare authority secures a private permissioned network for registered stakeholders, which only they have access to. Everyone will be working with additional security using a virtual private network connection to access to the registration system (VPN). At the time of registration, the patient will simply give registration information, such as name, social security number, address, and contact information. Additionally, all of the above will register with the regulating healthcare authority: the main physician, hospital, laboratory, pharmacy, researcher, and insurance. After they have completed the registration process, the public health authority verifies the record and provides a chaincode address. All parties have completed the registration process, and now, all transactions on the network are completed.

Figure 4 depicts the process involved in the hyperledger blockchain in the healthcare sector. Hyperledger fabric is a model based on a modular design that enables security, resilience, flexibility, and scalability. It offers plug-in implementation of diverse elements and adjusts with the complexity and delicacies which is present in the economic ecosystem. Among the basic ideas of fabric technology in the block diagram, the major components are listed as follows.

Chain codes:
It is currently written in Go language and is a self-executing program (similar to smart contracts).

Channels:
It is a private 'subnet' of communication among particular members (or hospitals) of the network, with the goal of confidential transaction.

Ordering service:
It ensures the constancy and scheduling of transactions.

Endorsement policy:
It comprises the set of rules employed for allowing a node in deciding if the transactions are approved or not.

Application SDK:
The software development kit allows peers to communicate with in the network.

Endorsing peers:
It approves transactions earlier to commitment based on the endorsement policy defined in the chain codes.

Committing peers:
It gets the blocks from the ordering service for validating them and updates the status of data in the State DB and the ledger.

Disease diagnosis process

To diagnose the disease from the healthcare records, the VAE model is applied in which the existence of disease can be accurately identified. Before applying the VAE model, min—max data normalization process takes place to normalize the data. Then, VAE model is applied to determine the proper class labels to the applied health records. The VAE network presents a probabilistic perception in the latent parameter space. An essential objective of the VAE is to utilize the latent parameter z to describe the sharing of the novel dataset $X = \{x_i\}_{i=1}^{N}$. They consider that the qualified sharing of latent parameter z depends on Gaussian distribution. Figure 5 shows the structure of VAE. This concept demonstrates that the hidden parameter z fulfills the Gaussian distribution that could create information fulfilling some distribution via NN. By enhancing the created variable θ, the latent parameter z creates a dataset $X = \{\widehat{x_i}\}_{i=1}^{N}$ which is equivalent to the actual data $\widehat{X} = \{x_i\}_{i=1}^{N}$. This implies that it would exploit the marginal probability $p_\theta(x)$ [32]

$$p_\theta(x) = \int p_\theta(z)\, p_\theta(x|z) dz, \quad \text{with } z \sim N(0,\ I)\ . \tag{14}$$

The actual true posterior density $p_\theta(z|x)$ is intractable, and for solving this issue, the VAE presents an identification module $q_\phi(z|x)$ to estimate the uncertain true posterior $p_\theta(z|x)$. The VAE calculates the comparison between identification module $q_\phi(z|x)$ and true posterior distribution $p_\theta(z|x)$ by Kullback–Leibler (KL) divergence

$$\log p_\theta\left(x^{(i)}\right) = D_{KL}\left(q_\phi\left(z|x^{(i)}\right)||p_\theta\left(z|x^{(i)}\right)\right) + L\left(\theta, \emptyset; x^{(i)}\right). \tag{15}$$

Since the KL divergence is generally greater than zero

$$\log p_\theta(x^{(i)}) \geq L\left(\theta,\ p; x^{(i)}\right).$$

This equation $\left(\theta, \left(p; x^{(i)}\right)\right)$ named (i.e., variational) low bound on peripheral probability of data point i, is stated as follows:

$$\begin{aligned} L\left(\theta,\ \left(\phi; x^{(i)}\right)\right. &= -D_{KL}\left(q_\phi\left(z|x^{(i)}\right)\ p_\theta\ (z)\right) \\ &+E_{q_{\phi(z|^{(i)})}}\left[\log\ p_\theta\left(x^{(i)}|z\right)\right]. \end{aligned} \tag{16}$$

To enhance $\log p_\theta(x)$, the variational lower bound on the marginal probability establishes the whole optimization purpose of VAE. The initial term on right side of Eq. (16) matches the regularization term and a negative reconstruction error in the autoencoder. Thus, $q_\phi(z|x^{(i)})$ is denoted as probabilistic encoder with variational variable and (ϕ, and $p_\theta(x^{(i)}|z)$ is denoted as probabilistic decoder with generation variable θ. The conditional distribution $p_\theta(x^{(i)}|z)$ is commonly given under a Bernoulli/Gaussian distribution

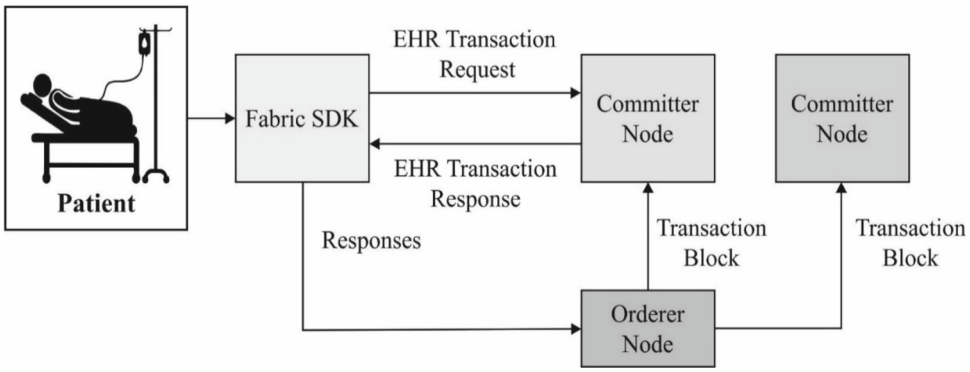


Fig. 4 Hyperledger blockchain in healthcare

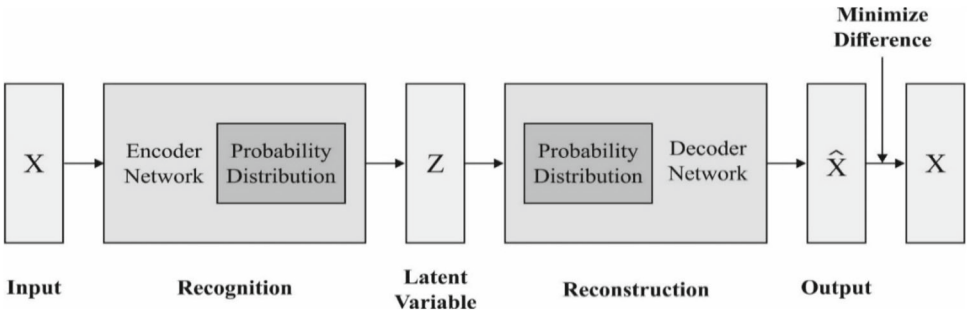


Fig. 5 Architecture of VAE model

Table 2 Dataset description

Description	Heart Statlog	Pima Indian Diabetes	EEG Eyestate
No. of instances	270	768	14,980
No. of attributes	13	8	15
No. of class	2	2	2
No. of samples in class 1	150	268	82,527
No. of samples in class 2	120	500	6723
Data source	[34]	[35]	[36]

Table 3 Result analysis of proposed GTOA-SIMON-based encryption and decryption time analysis (sec) with security level

Data size (%)	Encryption time	Decryption time	Security level
Heart Statlog dataset			
20	06.82	06.70	93.28
40	14.29	12.66	93.56
60	19.67	16.83	94.90
80	26.12	22.09	94.76
100	31.88	24.87	93.52
Pima Indian Diabetes dataset			
20	09.63	08.35	92.78
40	17.36	16.45	94.82
60	27.40	26.08	93.80
80	36.51	35.21	94.76
100	47.08	44.01	95.87
EEG Eyestate dataset			
20	21.73	19.82	93.70
40	40.87	39.06	95.74
60	61.63	59.61	94.80
80	79.41	76.54	93.73
100	95.38	93.03	96.84

[33]. In this research, the input data of network are patient healthcare records instead of binary data, and the distribution $p_\theta(x^{(i)}|z)$ is considered to be Gaussian. Later, they estimate stochastic gradient variational Bayes estimator of variational lower bound $(\theta, \phi, x^{(i)})$. When presenting the identification module $q_\phi(z|x^{(i)})$, they utilize reparameterization method where z denotes continuous arbitrary parameter and $z \sim q_\phi(z|x^{(i)})$ indicates conditional distribution, with the summary of an auxiliary noise variable $\varepsilon \sim p(\varepsilon)$. Here, $p(\varepsilon)$ has a recognized marginal probability distribution. Employing a distribution conversion on $q_\phi(z|x^{(i)})$ leads to $\tilde{z} = g_\phi(\varepsilon, x^{(i)})$. They consider $q_\phi(z|x^{(i)})$ that fulfills a Gaussian distribution where $(z) = N(z; 0, I)$. The calculation $q_\phi(z|x^{(i)}) = N(z; u, \sigma^2 I)$, regularization term is given by

$$D_{KL}\left(q_\phi\left(z|x^{(i)}\right) || \, p\,(z)\right) = \frac{1}{2}\sum_{j=1}^{j}\left(1 + \log\left(\sigma^{(i)^2}\right) - u^{(i)^2} - \sigma^{(i)^2}\right), \tag{17}$$

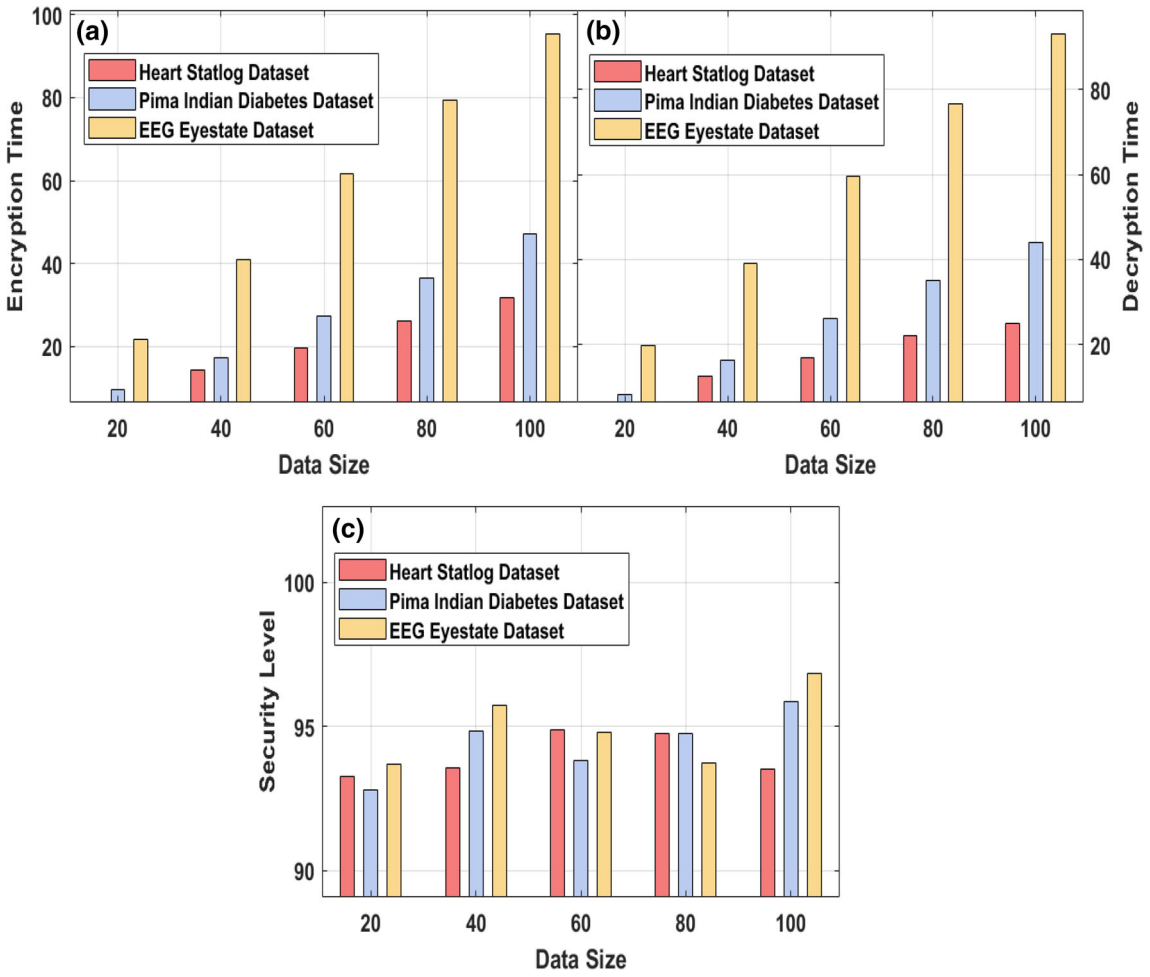


Fig. 6 Result analysis of GTOA-SIMON model on three datasets

where j represents dimension of z. While resolving the reconstruction term, by Monte Carlo evaluation, we attain the succeeding equation

$$E_{q_{\phi(z|^{(i)})}}\left[\log p_\theta\left(x^{(i)}|z\right) = \frac{1}{L}\sum_{l=1}^{L}\log\left(p\left(x^{(i)}|z^{(ii)}\right)\right)\right]. \tag{18}$$

Based on VAE principle, the data reconstruction is assumed and the root cause of exception is examined $a\Psi$. In training stage of the module, the whole module is trained with regular healthcare records. Therefore, if the modules obtain better disease diagnostic outcome on the tested data, the decoder and encoder of the module would demonstrate on the reconstructed data of hidden parameter z.

Performance validation

In this section, the performance of the proposed HBESDM-DLD technique is validated using three medical datasets, namely, Heart Statlog, Pima Indian Diabetes, and EEG Eyestate dataset. The first Heart Statlog dataset includes a set of 270 instances with 13 attributes. The second PIMA Indians diabetes dataset contains 768 instances with 8 attributes. Finally, the EEG Eyestate dataset contains 14,980 instances with 15 attributes. The detailed dataset is given in Table 2.

A detailed security analysis of the GTOA-SIMON technique on three different datasets is given in Table 3 and Fig. 6. From the table values, it is clear that the GTOA-SIMON technique has achieved improved security with encryption time, decryption time, and security level. For instance, on heart statlog dataset with 20% data size, the GTOA-SIMON technique achieves an encryption time of 6.82 s, decryption time of 6.70 s, and security level of 93.28%. Followed by, with 100% of data size, the GTOA-SIMON technique obtains an encryption time of 31.88 s, decryption time of 24.87 s, and security level of 93.52%. Similarly, on PIMA Indian diabetics dataset with 20% data size, the GTOA-SIMON technique resulted to an encryption time of 9.63 s, decryption time of 8.35 s, and security level of 92.78%. Next, with 100% of data

size, the GTOA-SIMON technique achieves an encryption time of 47.08 s, decryption time of 44.01 s, and security level of 95.87%. Likewise, on EEG EyeState dataset with 20% data size, the GTOA-SIMON technique resulted to an encryption time of 21.73 s, decryption time of 19.82 s, and security level of 93.70%. Next, with 100% of data size, the GTOA-SIMON technique achieves an encryption time of 95.38 s, decryption time of 93.03 s, and security level of 96.84%.

For ensuring the improved security performance of the GTOA-SIMON technique, a brief comparative study takes place in Table 4 and Fig. 7. From the results, it is noticed that the Blowfish technique has achieved the least security level of 90.81%. At the same time, the ECC and RSA models have obtained slightly increased security levels of 91.03% and 91.67%, respectively. Simultaneously, the SIMON and SC technique has attained reasonable security levels of 94.29% and 93.71%, respectively. However, the GTOA-SIMON technique has accomplished significant performance with the maximum-security level of 94.46%.

A detailed comparative result analysis of the HBESDM-DLD with existing techniques on Heart Statlog dataset is displayed in Table 5 and Fig. 8 [37, 38]. From the results, it is evident that RT model has the least outcome with the minimal accuracy of 0.76. Similarly, the J48 model shows slightly enhanced performance with the accuracy of 0.77. Next, the

Table 4 Comparative analysis of various encryption techniques with GTOA-SIMON-based security level (%)

Methods	Security level
GTOA-SIMON	94.46
SIMON	94.29
Signcryption (SC)	93.71
ECC	91.03
RSA	91.67
Blowfish	90.81

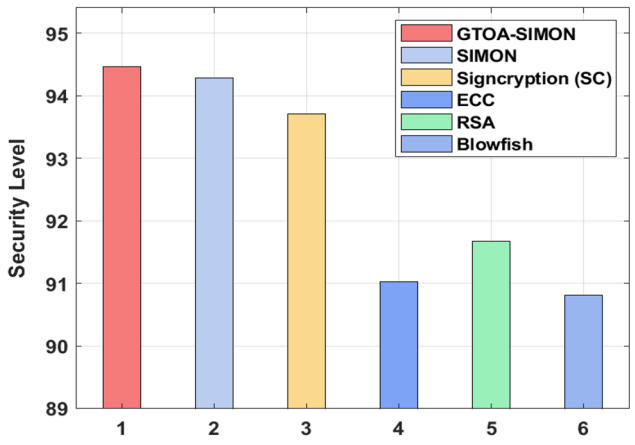


Fig. 7 Security level analysis of GTOA-SIMON model

Table 5 Performance evaluation of existing with proposed HBESDM-DLD method on Heart Statlog dataset

Methods	Precision	Recall	Accuracy	F-Score	Kappa
HBESDM-DLD	0.97	0.98	0.98	0.98	0.97
EEPSOC-ANN	0.95	0.97	0.95	0.97	0.94
DOD-GBT	0.95	0.97	0.96	0.96	0.93
GBT	0.96	0.94	0.95	0.95	0.90
J48	0.73	0.74	0.77	0.74	0.53
Random Tree	0.74	0.73	0.76	0.74	0.52
RBFNetwork	0.80	0.83	0.84	0.82	0.68

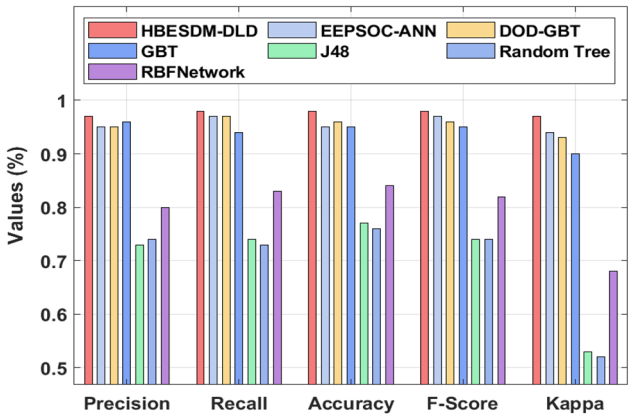


Fig. 8 Comparative analysis of HBESDM-DLD method on Heart Statlog dataset

RBF Network model has depicted moderate outcome with the accuracy of 0.84. Simultaneously, the EEPSOC-ANN and GBT models have exhibited reasonable accuracy of 0.95 and 0.95, respectively. Though the DOD-GBT model has tried to attain optimal accuracy of 0.96, the presented HBESDM-DLD technique has outperformed all the other approaches with the maximal accuracy of 0.98.

A detailed comparative result analysis of the HBESDM-DLD with existing techniques on Pima Indian Diabetes dataset is shown in Table 6 and Fig. 9 [39]. From the results, it is evident that Voted Perceptron approach has the least outcome with the minimal accuracy of 0.67. Likewise, the DT model has slightly enhanced performance with the accuracy of 0.74. Next, the LogitBoost model has depicted moderate result with the accuracy of 0.74. Simultaneously, the LR model has exhibited reasonable accuracy of 0.77. Though the MR-OGBT model has tried to attain optimal accuracy of 0.89, the presented HBESDM-DLD technique has outperformed all the other techniques with the higher accuracy of 0.95.

A detailed comparative result analysis of the HBESDM-DLD with existing techniques on EEG EyeState dataset is displayed in Table 7 and Fig. 10 [40, 41]. Results show that RT model with lowest accuracy of 0.76 is least successful.

Table 6 Performance evaluation of existing with proposed HBESDM-DLD method on Pima Indian Diabetes dataset

Methods	Precision	Recall	Accuracy	F-Score	Kappa
HBESDM-DLD	0.94	0.96	0.95	0.93	0.93
MR-OGBT	0.92	0.91	0.89	0.91	0.75
LR	0.88	0.79	0.77	0.83	0.47
Voted Perceptron	0.92	0.68	0.67	0.78	0.14
LogitBoost	0.85	0.78	0.74	0.81	0.41
DT	0.81	0.79	0.74	0.80	0.42

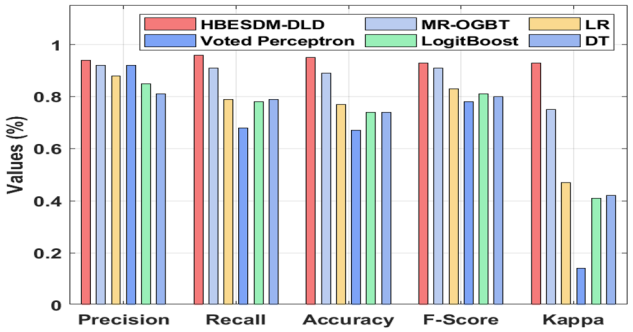


Fig. 9 Comparative analysis of HBESDM-DLD method on Pima Indian Diabetes dataset

Table 7 Performance evaluation of existing with proposed HBESDM-DLD method on EEG EyeState dataset

Methods	Precision	Recall	Accuracy	F-Score	Kappa
HBESDM-DLD	0.93	0.95	0.93	0.93	0.92
DE-LSTM	0.90	0.89	0.90	0.89	0.87
RS-LSTM	0.89	0.89	0.90	0.87	0.85
SA-LSTM	0.86	0.86	0.86	0.84	0.69

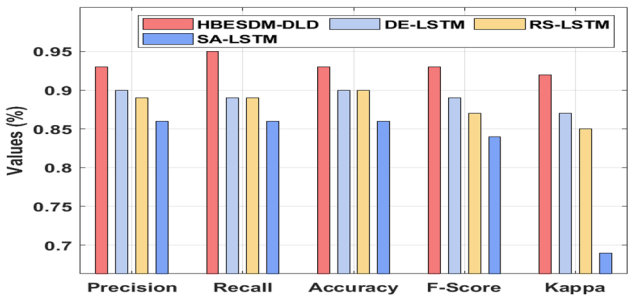


Fig. 10 Comparative analysis of HBESDM-DLD method on EEG Eye-State dataset

At the same time, a better performance with 0.86 of accuracy is shown by SA-LSTM. Simultaneously, the RS-LSTM and DE-LSTM techniques have exhibited reasonable and similar accuracy of 0.90 each, respectively. The presented HBESDM-DLD technique has outperformed all the other models with the maximal accuracy of 0.93.

From the above-mentioned result analysis, it is apparent that the HBESDM-DLD technique has accomplished the maximum secrecy with significant detection performance. Therefore, it can be employed in real-time environment for secure transmission of health records and the corresponding diagnostic process.

Conclusion

This paper has developed a novel HBESDM-DLD model for secure data transmission and diagnostic process. The presented model involves distinct stages of operations such as SIMON block cipher-based encryption, GTOA-based optimal key generation, hyperledger blockchain-based secure data management, and VAE-based diagnosis. The inclusion of GTOA in the key generation process results in enhanced security level of the health record transmission process. Meanwhile, the hyperledger blockchain enables secure health record management, which permits the patient to access or revoke access to any physician or medical organization. At last, the VAE-based diagnostic process is performed to determine the existence of the diseases. The HBESDM-DLD experimental result is investigated using benchmark medical dataset and the results are examined by various performance measures. The experimental result indicates that the HBESDM-DLD methodology is superior to state-of-art methods. In future, the presented HBESDM-DLD technique can be extended to the use of metaheuristic optimization-based hyperparameter optimizer and learning rate schedules for VAE model.

Declarations

Conflict of interest The authors declare that they have no conflict of interest. The manuscript was written through contributions of all authors. All authors have given approval to the final version of the manuscript.

References

1. Naz M, Al-zahrani F, Khalid R, Javaid N, Qamar A, Afzal M, Shafiq M (2019) A secure data sharing platform using blockchain and interplanetary file system. Sustainability 11(24):7054. https://doi.org/10.3390/su11247054
2. Hasselgren A, Kralevska K, Gligoroski D, Pedersen S, Faxvaag A (2020) Blockchain in healthcare and health sciences—a scoping review. Int J Med Informatics 134:104040. https://doi.org/10.1016/j.ijmedinf.2019.104040
3. Zhang X, Poslad S (eds) (2018) Blockchain support for flexible queries with granular access control to electronic medical records (EMR). Institute of Electrical and Electronics Engineers Inc
4. Sun Y, Zhang R, Wang X, Gao K, Liu L (eds) A decentralizing attribute-based signature for healthcare blockchain. In: 27th International conference on computer communication and networks (ICCCN), 30 July 2018–2 Aug. 2018
5. Abu-elezz I, Hassan A, Nazeemudeen A, Househ M, Abd-alrazaq A (2020) The benefits and threats of blockchain technology in healthcare: a scoping review. Int J Med Informatics 142:104246. https://doi.org/10.1016/j.ijmedinf.2020.104246
6. Li H, Zhu L, Shen M, Gao F, Tao X, Liu S (2018) Blockchain-based data preservation system for medical data. J Med Syst. https://doi.org/10.1007/s10916-018-0997-3
7. Zhang P, White J, Schmidt D, Lenz G (2017) Applying Software Patterns to Address—Interoperability in Blockchain-based Healthcare Apps. arXiv preprint at arXiv:170603700
8. Passerat-Palmbach J, Farnan T, Miller R, Gross MS, Flannery HL, Gleim B (2019) A blockchain-orchestrated federated learning architecture for healthcare consortia. arXiv preprint at arXiv:1910.12603.
9. Nguyen DC, Pathirana PN, Ding M, Seneviratne A (2021) A cooperative architecture of data offloading and sharing for smart healthcare with blockchain. arXiv preprint at arXiv:2103.10186
10. Al Mamun A, Jahangir MUF, Azam S, Kaiser MS, Karim A (2021) A combined framework of interplanetary file system and blockchain to securely manage electronic medical records. In: Proceedings of international conference on trends in computational and cognitive engineering. Springer, Singapore, pp 501–511
11. Bisogni C, Iovane G, Landi R, Nappi M (2021) ECB2: a novel encryption scheme using face biometrics for signing blockchain transactions. J Inf Secur Appl 59:102814. https://doi.org/10.1016/j.jisa.2021.102814
12. Yates T (2020) Enhancing healthcare information sharing with blockchain technology. Open Sci J. https://doi.org/10.23954/osj.v5i2.2400
13. Fan K, Wang S, Ren Y, Li H, Yang Y (2018) MedBlock: efficient and secure medical data sharing via blockchain. J Med Syst. https://doi.org/10.1007/s10916-018-0993-7
14. Hylock R, Zeng X (2019) A blockchain framework for patient-centered health records and exchange (HealthChain): evaluation and proof-of-concept study. J Med Internet Res 21(8):e13592. https://doi.org/10.2196/13592
15. Sun J, Ren L, Wang S, Yao X (2020) A blockchain-based framework for electronic medical records sharing with fine-grained access control. PLoS ONE 15(10):e0239946. https://doi.org/10.1371/journal.pone.0239946
16. Chen Y, Ding S, Xu Z, Zheng H, Yang S (2018) Blockchain-based medical records secure storage and medical service framework. J Med Syst. https://doi.org/10.1007/s10916-018-1121-4
17. Ekblaw, Ariel et al (2016) A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data
18. Vora J, Nayyar A, Tanwar S, Tyagi S, Kumar N, Obaidat MS, Rodrigues JJ (2018) BHEEM: a blockchain-based framework for securing electronic health records. In 2018 IEEE globecom workshops (GC Wkshps). IEEE, pp. 1–6
19. Guo R, Shi H, Zhao Q, Zheng D (2018) Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. IEEE Access 6:11676–11686
20. Guo H, Li W, Nejad M, Shen CC (2019) Access control for electronic health records with hybrid blockchain-edge architecture. In: 2019 IEEE international conference on blockchain (blockchain). IEEE, pp 44–51
21. Sharma Y, Balamurugan B (2020) Preserving the privacy of electronic health records using blockchain. Proc Comput Sci 173:171–180
22. Zhang L, Zou Y, Wang W, Jin Z, Su Y, Chen H (2021) Resource allocation and trust computing for blockchain-enabled edge computing system. Comput Secur 105:102249
23. Chen J, Ma X, Du M, Wang Z (eds) A blockchain application for medical information sharing. In: IEEE International symposium on innovation and entrepreneurship (TEMS-ISIE), 30 March 2018–1 April 2018
24. Wang W, Xu H, Alazab M, Gadekallu TR, Han Z, Su C (2021) Blockchain-based reliable and efficient certificateless signature for IIoT devices. In: IEEE transactions on industrial informatics
25. Wang W, Huang H, Zhang L, Su C (2020) Secure and efficient mutual authentication protocol for smart grid under blockchain. Peer-to-Peer Netw Appl. https://doi.org/10.1007/s12083-020-01020-2
26. Rajadurai S, Alazab M, Kumar N, Gadekallu TR (2020) Latency evaluation of SDFGs on heterogeneous processors using timed automata. IEEE Access 8:140171–140180. https://doi.org/10.1109/ACCESS.2020.3013013
27. Shankar K, Elhoseny M (2019) An optimal light weight cryptography—SIMON block cipher for secure image transmission in wireless sensor networks. In: Secure image transmission in wireless sensor network (WSN) applications. Springer, Cham, pp 17–32
28. Zhang Y, Jin Z (2020) Group teaching optimization algorithm: a novel metaheuristic method for solving global optimization problems. Expert Syst Appl 148:113246. https://doi.org/10.1016/j.eswa.2020.113246
29. Drescher D (2017) Blockchain basics: a non-technical introduction in 25 steps. Apress
30. Fernandes A, Rocha V, da Conceição AF, Horita F (2020) Scalable architecture for sharing EHR using the hyperledger blockchain. In: 2020 IEEE international conference on software architecture companion (ICSA-C). IEEE, pp 130–138
31. Stamatellis C, Papadopoulos P, Pitropakis N, Katsikas S, Buchanan WJ (2020) A privacy-preserving healthcare framework using hyperledger fabric. Sensors 20(22):6587
32. Doersch C (2016) Tutorial on Variational Autoencoders. 1606.05908
33. Luo Z, Xiong Y, Zuo R (2020) Recognition of geochemical anomalies using a deep variational autoencoder network. Appl Geochem 122:104710. https://doi.org/10.1016/j.apgeochem.2020.104710
34. http://archive.ics.uci.edu/ml/datasets/statlog+(heart)
35. https://www.kaggle.com/uciml/pima-indians-diabetes-database
36. https://archive.ics.uci.edu/ml/datasets/EEG+Eye+State
37. Song W (2020) A new method for refined recognition for heart disease diagnosis based on deep learning. Information 11(12):556. https://doi.org/10.3390/info11120556
38. Gaona A, Arini P (2020) Deep recurrent learning for heart sounds segmentation based on instantaneous frequency features. Elektron 4(2):52–57. https://doi.org/10.37537/rev.elektron.4.2.101.2020

39. Vu Q, Truong V, Thai H (2021) Machine learning-based prediction of CFST columns using gradient tree boosting algorithm. Compos Struct 259:113505. https://doi.org/10.1016/j.compstruct.2020.113505
40. Nizami Huseyn E (2020) Application of deep learning technology in disease diagnosis. Nat Sci 04(05):4–11. https://doi.org/10.36719/2707-1146/05/4-11
41. Maiorana E (2020) Deep learning for EEG-based biometric recognition. Neurocomputing 410:374–386. https://doi.org/10.1016/j.neucom.2020.06.009