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

**Abstract**

Electronic medical records are being created in large amounts as a result of recent advances in the healthcare sector (EHRs). The data owner can manage his or her data and distribute it with certain individuals thanks to the EHR system. Data security and diagnostic procedures are challenging to maintain because of the enormous volume of data in the healthcare system. The HBESDM-DLD model, which combines secure medical data management with deep learning (DL)-based diagnosis to address these problems, is developed in this study.The provided architecture includes many phases of activities such encryption, the development of the best keys, secure data management using the Hyperledger blockchain, and diagnostics. The shown model enables the user to manage data access, allow hospital administrators to read and write data, and notify emergency contacts. It uses the SIMON block cypher algorithm for encryption. A group teaching optimization algorithm (GTOA) is used for the SIMON technique's best key generation at the same time in order to increase its effectiveness. Moreover, the exchange of medical data occurs via the multi-channel hyperledger blockchain, which uses a blockchain to store information about patient visits as well as linkages to EHRs that are stored in other databases.Finally, a diagnostic model based on variational autoencoders (VAE) is used to detect the presence of the illnesses once the data have been decrypted at the receiving end. Using a benchmark medical dataset, the HBESDM-DLD model's performance is validated, and the results are examined using a variety of performance metrics. The experimental data demonstrates the superiority of the HBESDM-DLD methodology over state-of-the-art approaches.

**Introduction**

To effectively handle patient information, the personal health record (PHR) system is an important healthcare industry resolution. The PHR system enables data exchange with healthcare professionals and aids in the foretelling of health issues. It holds extremely sensitive data and stores health-related information. A few careless adjustments or revisions of certain PHR information might have catastrophic repercussions. Hence, confidentiality becomes a key component of PHR systems. The PHR system needs a tamper-resistant element to function properly. When a person's lifetime health-related data can be gathered and kept in a way that makes it impossible for it to be tampered with, it significantly improves the quality of their personal protection healthcare. Blockchain's immutability, backup, and cryptographic verifiability features might make it a useful tamper-resistant storage option for the PHR system.The crucial step in obtaining the greatest advantages from an innovative study is data sharing. It is crucial to understand the 3 Ws, or where, what, and when. Before beginning the process of data exchange, these inquiries should be precise. There aren't many operating scopes, and the owner of the data set must offer incentives and rewards. This study demonstrates safe data exchange while utilising blockchain's advantages. Blockchain, a distributed ledger, is a new development in the IT industry.

According to a Silicon Valley specialist, the consensus technique is regarded as an important and vital invention. The removal of unauthorised parties achieves trust, which is a key feature of blockchain technology. Blockchain is currently used in many industries, including health care, IoT, cloud computing, information security, data trade, etc. The misunderstanding and abuse of information are the key difficulties in this data sharing.

In general, the cloud server is a centralised authority that stores a vast amount of data. A technology called decentralised storage enables data to be kept on several network nodes as a shared ledger. The difficulty is the network nodes' processing and storage limitations. With a storage system based on a decentralised structure and IPFS, data accessibility is ensured. The data owners do not have full access to the data in the architecture as it is now set up. The owner is often excluded from data sharing. For instance, when escrow is independently responsible for payment settlements and data delivery, the owner is a passive entity. Without blockchain, it is extremely difficult to guarantee fund transparency, without which it would be impossible to guarantee fair money distribution.

In this scenario, blockchain might offer network nodes transparency and trust for a fair distribution of the money received from the data requestor. If a customer is paying to get the content, on the other hand, integrity and quality of the information may not have partnered.

An exclusive remedy is offered to deal with these issues. In this circumstance, the owner (i.e., patient) manages the dissemination of the health record by keeping out other parties. Information would not be disclosed to other parties if the data owner fixed the access rules. With federated learning (FL), businesses pool their data to create an integrated, complex machine learning model that works as a closed-loop system. In the near future, companies will be able to accomplish amazing things like enhancing consumer data privacy, data security, data-access rights, and access to heterogeneous data thanks to their increased capacity to have deep customer insights. FL enables machine learning algorithms to gain real experience with a variety of distinct datasets that are all spread out across different locations. This method makes it easier to create models that different businesses may collaborate on without having to share sensitive information. The following are some of this article's significant contributions.

* With the use of deep learning (DL)-based diagnosis, the proposed model creates a novel hyperledger blockchain-enabled secure medical data management (HBESDM-DLD) paradigm.
* It enables the user to manage data access, provide hospital administrators access to read and write data, and notify emergency contacts.
* The SIMON block cypher technology is used in the proposed HBESDM-DLD model to encrypt the medical records.
* By combining the best key generation process with the group teaching optimization algorithm (GTOA), the efficacy of the SIMON approach may be improved.
* Additionally, the hyperledger blockchain's multi-channel functionality is used for the exchange of medical records.
* The suggested methodology incorporates blockchain technology and the federated learning (FL) idea. A variational autoencoder (VAE)-based diagnostic model is used in addition to the data decryption procedure for accurate illness diagnosis.
* The experimental findings of the HBESDM-DLD model are evaluated using a variety of performance indicators on benchmark medical datasets.

**Related Works**

This section examines the most cutting-edge blockchain-enabled healthcare systems that have recently been created, with a focus on secure medical data transfer. Nguyen et al.presented a new hybrid strategy using edge cloud and blockchain for data dumping and sharing in healthcare. An efficient data offloading system is first shown, with IoT healthcare data being transmitted to a nearby edge server for privacy-conscious data processing. The next step is leveraging blockchain to connect a data sharing system with data exchange between healthcare clients. In particular, an intelligent contract management offers a trustworthy access control method for obtaining authentication to complete protected EHR distribution. Al Mamun et al.proposed an IPFS-integrated blockchain solution architecture for EMR in the medical industry. It provides access guidelines to various customers and intends to develop a blockchain for EMR. The architecture that is being described safeguards individual privacy while allowing authorised parties, such as healthcare providers, appropriate access to medical data. Bisogni et al.a novel encryption technique that is specifically intended for signing and approving transactions in digital/intelligent contract systems. FaceNet and CNN have jointly developed a biometric key that uses face recognition. Yates [12] presented a brand-new hybrid approach to edge cloud and blockchain-based data offloading and sharing for the healthcare industry. When IoT healthcare data are offloaded in a nearby edge server for processing with privacy attention, an effective data offloading system is first envisioned. The next step is to create a data sharing system for leveraging blockchain to enable data exchange across healthcare facilities. An intelligent contract management primarily introduces a trustworthy access control system for accessing authentication to provide protected EHR distribution.By combining the strengths of blockchain and CC, Huang and Lee [13] were able to establish a privacy protection solution for medical data. This system presents CC and offers a service for blockchain nodes with CC servers where it collects, examines, processes, and preserves medical data in the identity authentication interface and addresses insufficient computing capabilities of a small number of blockchain nodes for verifying consistency and authenticity.HealthChain is a brand-new patient-centered blockchain architecture that was unveiled by Hylock and Zeng [14]. The goal is to improve data curation, controlled data transmission, and person appointment on an interoperable, secure platform. A person can also get a private and public key pair for a cryptographic identity. The blockchain stores the public keys, which are used to protect and validate transactions. The planned system also makes use of revocable intelligent contracts with proxy re-encryption (PRE) to share data while maintaining privacy and secrecy.Sun et al. [15] demonstrated a searchable distributed electronic medical record system that makes use of blockchain technology and intelligent contracting. To ensure the validity and integrity of the electronic medical data, they first perform hash calculations on it and deposit an equal value on then blockchain. The distributed storage technology, IPFS, is then used to encrypt it. Nonetheless, it is best in minimizing the load from data storage and more often accessing to blockchain. This process might resolve the central data storage of the server of numerous medical organizations. After that, a smart contract that uses the keyword search rather than a central third party is employed to understand the encrypted keyword index data stored on the Ethereum blockchain.In order to ensure that attributes can comply with the access rules for decrypting the encrypted data, they also used an attribute-based encryption system. Chen et al.[16] created a cloud-based and blockchain-based storage system for handling individual medical data. A service architecture for exchanging medical records is also shown. None of the parties involved in the shared storage and sharing systems are in a position to influence the process or rely on any third parties. An Identity Mixer and distributed ledger technology-based new EHR management system named PREHEALTH have been suggested (Idemix). a demonstration of a proof-of-concept that uses the permissioned blockchain architecture to mimic the interaction between apps and permissioned blockchains. It is conceivable to develop a system for preserving records while protecting patient privacy and unlikability. Results from the experiments demonstrate the system's viability for wide-scale application.Ekblaw et al. implemented [17] In addition to facilitating data exchange, MedRec makes use of blockchain technologies to provide secure authentication, confidentiality, and accountability. The system's modular design interfaces with the services providers' current local data storage options, enabling interoperability and enhancing the system's flexibility and use. We provide prizes in the form of bitcoin to encourage academics, public health professionals, and others to join the network as blockchain "miners." With this in place, miners may get rewards based on anonymized data while also using Proof of Work to support and maintain the network. In addition to providing vast data to researchers and involving patients and physicians in the decision of whether to make information publicly available, MedRec also empowers data economics. Hyperledger blockchain has an influence on the summary of suggested solutions, as seen in Table 1.

**Literature Survey**

Vora et al. [18] in this paper propose a blockchain-based method for effectively managing and preserving EHRs. This provides a safe and effective way to obtain medical data while also helping to maintain patient privacy.

for service suppliers, clients, and other stakeholders. Our study intends to assess how well the framework can satisfy the needs of patients, healthcare providers, and third parties. It also attempts to determine how well the framework manages to maintain privacy and security while incorporating the burgeoning healthcare 4.0.

This is significant since it addresses both the escrow issue and the blockchain's distributed data storage model [19]. By spreading the pseudorandom function seeds across the authorities and guaranteeing that no more than N - 1 of them are corrupt, the protocol prevents collusion attack By using the computational bilinear Diffie-Hellman assumption, this signature approach is formally demonstrated to be secure. This study provides a hybrid architecture for access management of EHR data that makes use of both blockchain and edge nodes [20]. A blockchain-based controller that simultaneously functions as a tamper-proof log of access events is used to enforce the identification and access control limitations. The second is that EHR data is stored on off-chain edge nodes, which work with access control logs based on blockchain technology to offer attribute-based access control on EHR data using ALFA, a predetermined set of characteristics. To make electronic health records (EHRs) safer and more private, Sharma et al. [21] are now creating a system that uses blockchain technology to deploy EHRs. This technology will control information access using decentralisation and cryptography. Also, it maintains a balance between data accessibility and privacy. The main goal of our study is to shed new light on the issues with data security and privacy in electronic healthcare. We develop a distributed system comprised of current EHRs that use consortium blockchain using hyperledger fabric [22]. Peers maintain the blockchain that houses all patient data using the same ledger that peers use to record the address of a patient record in an EHR [23]. A local certificate authority, which collaborates with other certificate authorities to build a network channel, issues each patient's unique certificate. We use a proxy re-encryption method to protect patients' privacy when their data is sent. With the help of a centralised service provider, the Federated Learning setup uses machine learning with clients like mobile devices or large businesses to train a model collectively [24]. The participants in the learning process maintain the decentralised data. FL is committed to gathering the appropriate data while reducing the numerous privacy risks and expenses connected with the application of centralised standard machine learning and data science methodologies. The paper highlights recent developments and offers a comprehensive list of unresolved problems and difficulties, all spurred on by the sharp rise in FL research.Wang et al.[25] demonstrated it through the design and implementation of a novel privacy-preserving inference information flow. The computation time of inference and the payload size of activation signals are significantly impacted by the model's division farther down the computation chain. More model secrecy results from this, albeit at the expense of longer computation times.Rajadurai et al. [26] employ a technique to keep an SDF graph's optimal throughput while calculating the latency of a static schedule for a specific unfolding factor on a heterogeneous multiprocessor platform.

***TABLE 1***

The execution platform and synchronous data flow graph in the system model are both made up of timed automata. The final result is defined using the UPPAAL model checker.

**The proposed HBESDM-DLD model**

The HBESDM-DLD model is depicted in Fig. 1 as it goes through several stages of operation, including encryption, optimum key generation, hyperledger blockchain-based secure data management, and diagnostics. The patient's health records are initially encrypted using the SIMON block cypher method and a GTOA-based optimum key generation method. The hyperledger blockchain, which has a global blockchain and several local blockchain for medical institutions, is also involved in the data encryption process. The patient grants or denies access to any doctor or medical facility. The authorised user can decode the encrypted data and obtain the genuine medical records. The VAE-based diagnostic procedure is used to identify any illnesses at the very end of the process.

**Data encryption process**

Hash functions, block cyphers, validated decryption, and encryption modelling procedures are examples of low weight cryptographic techniques. For the purpose of managing secure healthcare records, block cyphers are used in this study. Beginning with a more advanced advanced encryption standard, lightweight cypher development occurs (AES). There are now several cyphers accessible, including the RECTANGLE, SIMON, TWINE, KATAN, SPECK, and KLEIN cyphers. The performance of SIMON, a compact block cypher, is based on hash function and effectiveness when connected to hardware. Ten functions in this cypher family, including key size and block, have different structures for the two variables. The key for each block is different depending on the picture pixels. The SIMON block cipher's construction is shown in Figure 2. The block quantifies the variance between 32 and 128 bits, which roughly equates to 16. It carries a block of encrypted material and performs an action on a set size block of plain text [27]. The SIMON cypher has direct and nonlinear characteristics for studying security in relation to block size and data. The person might think about a tree for each difference in all rounds while employing a set of input variances, creating some of the potential output variances.

**FIG - 1**

**FIG - 2**

On the off-chance that the key qualities are extended to further rounds, people might make use of the robust structure of round capabilities. The SIMON key calendar develops the number of pixels valued in a picture while utilising the round reliability for key schedule characteristics. With the 15-round SIMON48 on the light block cypher, there is just one single key difference signal. This block cipher's quality was not designed to be perfect.The chosen optimizer generates the optimal result, and this approach's quality is assured to have the fewest active S-boxes.

Today, encryption, rounding, biting, and decryption are some of the key elements used in cypher modules for safe data transport. Fig. 3 shows how the SIMON cypher round function divides an input plaintext block (2n) into two words of equal size as an illustration (each one is n-bit).Each round function performs three left shifts and bitwise AND logic operations on the left half block. The round key is employed, and the right half block is XORed with the XOR result, as illustrated in Fig. 2. At the end of each round, the created value is written back to the left block while the left half value is transferred to the right block.This round operation is continuously performed as long as the total number of rounds for the implemented configuration stays the same. Eq-1 can be used to represent F. The equivalents of the SIMON cypher with 2n-bit blocks are as follows:

***EQ-1***

This cypher is referred to as having round keys and round functions. Such function is referred to as an iterated block cypher. The SIMON round capability for encryption is provided by

***EQ-2***

The data is decrypted using the inverse function, as illustrated in Eq (3)

***EQ-3***

The terms used in Eq. (3) are for the left-most word in a block, for the right-most word, and for the right-round key.

**HBESDM-DLD algorithm**

HBESDM-DLD secure medical record management algorithm 1.

***algorithm-1***

**Optimal key generation process**

The SIMON cypher generates entire round keys from the master key to provide key expansion. The early 128-bit master key is converted by the selected SIMON64/128 formation into round keys that are 32 bits in size. By combining the saved previous round keys (key word variable) with trustworthy and 1 bit round, it secures the round. The main task of expansion makes use of related tasks.

* Indicated by bitwise XOR is .
* Left circular shift, , by j bits and right circular shift, , by j bits.
* Round counter with continuous sequence and and j = 0, 1, 2, 3, 4
* Constants, the number of cypher rounds, and the round key (sub-key).
* Right bitwise rotation ROR, where c stands for the number of rotations, is determined by .

Eq-(4) provides the crucial expansion procedure.

***Eq-4***

To decrypt the data, an ideal key can be chosen from among the many created keys. The GTOA is used to optimise the value as minimum or maximum in order to choose the best key. A group teaching method is used to stimulate the GTOA being delivered. The goal is to increase the class's collective knowledge. Given the wide range of differences among pupils, it is difficult to carry out in real time.

***Fig. 3 Flowchart of GTOA***

They first take into account population, decision parameter, and fitness value relating to the students in order to alter this approach to be suited for optimization procedure [28]. Subsequently, a straightforward group teaching module is developed without losing generalizability. The approach achieves consensus via transaction witness and pseudorandom sortition. Throughput, latency, and latency three dimensions have been added to the formula to boost the algorithm's scalability. Using a consensus technique with strong scalability, low latency, high throughput, and decentralised properties is recommended.

The GTOA algorithm is used in this work to offer an enhanced hybrid consensus algorithm. Verifiable cryptographic sortition chooses the consensus node in a dynamic manner, allowing a large number of nodes to fairly participate in the consensus while assuring low latency and high throughput. The provided module is divided into four stages: capacity grouping, teacher allocation, student stage, and teacher stage. These are the four phases' definitions.

**Capability grouping stage**

The knowledge of complete classes is seen as a normal distribution with no loss of generalization. It is provided by

***Equation-5***

When x represents the value of the normal distribution function, u stands for the mean class knowledge, and for the standard deviation (SD). The assumption is that a good teacher will raise knowledge levels on average (u), but lower SD . The instructor must develop an effective teaching method for their pupils in order to achieve this goal. Every student is divided into two smaller groups according to their capacity to apply information in GTOA in order to demonstrate the group teaching characteristic without losing generalisation. The possibility that the SD of exceptional and typical groups may exceed the transmission of instructional events is stressed. Capability grouping, an active technique in GTOA that is carried out across a learning cycle, seeks to address this issue. Figure 3 depicts the GTOA flowchart.

**Teacher stage**

It means that each pupil learns something from their instructor that has to do with the decided-upon next rule. In the given GTOA, the instructor develops a variety of instructional tactics for both ordinary and exceptional groups.

**Teacher stage I**

The instructor focuses more on enhancing the knowledge of the exceptional group since they have a better capacity for knowledge adaptation. In particular, the teacher could make every effort to raise the average level of knowledge across all classes. Students' differing approaches to applying their information must also be taken into account. Hence, the excellent set of students may acquire information and become

***Equation-6***

***Equation-7***

***Equation-8***

where t signifies the current number of iterations, N is the number of students, and denotes the student's knowledge at the moment.

t, denotes the teacher's knowledge at time t. F is the teaching factor, denotes the knowledge that student i at time t acquired from their instructor; and a, b, and c designate arbitrary variables. represents the mean knowledge of such a group at time t. As created, F has a value of either one or two.

**Teacher stage II**

A teacher concentrates on the average group as opposed to the exceptional group by adhering to principles that tend to improve the pupils' knowledge from the perspective of individuals, taking into account their least capacity to adapt knowledge. The average-group learner may therefore acquire information in this way:

***Equation-9***

where d can represent any number between 0 and 1.

Moreover, individual student knowledge gaps are addressed in the following ways (using the smallest issue as an example):

***Equation-10***

**Student stage**

It covers the first and second phases of the third rule as mentioned. Individual students might acquire their information in two different ways during free time, such as by self-teaching and by connecting with other students who are provided by their teachers.

***Equation-11***

and show knowledge of student i at time t via learning from student stage and instructor, respectively, where e and g represent two arbitrary quantities in the range of zero and one.

The student j( j{1, 2,..., i -1, i + 1,..., N}) is picked at random. The following item and the third item from the right in Eq. (11), respectively, suggest learning from another student and self-teaching.

Also, it is addressed (using the smallest issue as an example) that each student may not acquire information via the student stage as follows:

***Equation-12***

And student i's knowledge at time t + 1 in the learning cycle is represented by .

**Teacher allocation stage:**

As per fourth rule, building a reasonable instructor allocation approach is necessary to boost the understanding of students. In GWO, wolf hunts are guided by the first three discovered optimal solutions. The instructor distribution in the proposed technique is given by

Equation 13

where xt first, xt second, and xt third represent first, second, and third optimal pupils, respectively, and is stimulated by hunting behaviour in GWO. Similar professors are distributed to the outstanding and average groups in order to hasten the convergence of the presented GTOA.

HYPERLEDGER BLOCKCHAIN:

In this study, federated learning(FL) method is utilised in the blockchain with ML(Machine Learning)based disease diagnostic model. Blockchain is a shared ledger implementation method. It provides decentralisation, appropriateness, security, accessibility, and all of the above. Data stored in the Blockchain can now be replicated across a number of machines, eliminating the single point of failure associated with a centralized server. While the data is accessible when needed, very few computers really malfunction. Integrity with data upkeep, preserving it from unwanted changes.

The capacity to track all stored data in blockchains is possible.

Finally, privacy allows the members to remain anonymous. Technically speaking, the blockchain is made up of a collection of well-ordered and trustworthy blocks of chain, each of which includes a header and stores data. The header is made up of several elements, including the previous block, the identification, and the signature. The identification represents an internationally distinctive value with a mathematical function that encloses each block of data. Chaining blocks is managed by the preceding block. A logical chain of connections would be created since each novel block in the chain would include the identifier value of the block before it. One of the open-source blockchains provided by the Hyperledger management is called Hyperledger Fabric. It seeks to create a decentralised setting. It involves committed peer, client, certificate authority, order, and endorser peer. Additionally, the components communicate through channels that have been set up to enable transactions in a private and hidden manner, dividing various application domains. There are two methods that the fabric certificate authority is in charge of. First, it ensures that different components (users or smart contracts) can use the specified system. Then, it verifies the component and grants permission to use it for a certain function (such as carrying out a transaction) or access another part as a result of the authorization. The chain sent by the system-generated channel must be continued by the committing peer. As a result, they maintain different blockchains for every channel that an individual has formed. Scalability and anonymity are provided by this ‘individual chain per channel’ method.

When compared to privacy, a component that lacks easy access to a network cannot access a chain from a committed peer connected to the channel. Scalability states that individual for each channel permits the exchange of various transactions and data stored with in various committed nodes, increasing the demanded amount where a node gets fulfilled and to raise quantity of data, thus enhancing the system's sustainability. Peers who are approving are in charge of two processes. The first step is to collect the transaction from the client. After that, it is examined using a smart contract system because the transaction contains a number of linked rules that must be adhered to. Two processes are carried out by gathering peers, such as obtaining consumer transactions and organising transactions for assessing the blockchain's dependability. As a result, every ordering peer on a given chain needs to attest that the transaction was added to the committing peers. It is claimed that even though a person may frequently visit identical medical facilities, this blockchain only records one visit. The EHR pertinent to the individual is stored on the blockchain for each medical facility (also known as the local blockchain). It is assumed that the medical facility maintains the minimal structure needed to operate the hyperledger network in order to put the blockchain.

A smart contract is a chaincode application in hyperledger fabric. It is typical practise to construct network-agreed business logic using chaincodes. The state that results from the generation of a chaincode belongs to that chaincode alone and is unavailable to other chaincodes. If you have the required authorization, you can call another chaincode. It is useful to think about the following two sorts of chaincode while discussing them: a chain of application-specific code for the entire system In general, chaincode is in charge of processing system-related transactions, including lifecycle management and policy configuration. Nonetheless, users have access to the system's chaincode API and are free to modify it as needed. Application states, such as digital assets or arbitrary data input, must be maintained on the ledger by the application chaincode. A chaincode begins with a package that contains metadata, which is used to ensure the consistency of the code and metadata, such as the name, version, and counterparty signatures. The software is installed automatically on the counterparties' local computers when the chaincode package has been loaded on the counterparties' network nodes. A registration function is carried out within the smart contracts (chaincode) for the private health authority designated by the fabric network administrator to administer and manage the fabric network in order to register the members. For enrolled parties, the healthcare authorities establishes a private, permissioned network to which only they have accessibility. A virtual private network connection will be used by everyone to access the registration system with added security (VPN). The patient will just provide enrollment data at the time of registration, including name, social security number, address, and contact details. Also, the principal physician, hospital, laboratory, pharmacy, researcher, and insurance will all register with the body that regulates the healthcare industry. The public health authority checks the record when they have finished the enrollment process and issues a chaincode address. The registration procedure has been finished by all parties, and all transactions on the network have been finished.

The hyperledger blockchain procedure in the healthcare industry is shown in Figure 4. The modular nature of the Hyperledger Fabric model offers security, resilience, flexibility, and scalability. It provides plug-in implementation of a variety of components and adapts to the economic ecosystem's complexity and subtleties. The main components of the block diagram's fundamental fabric technology concepts are as following.

**Chain codes:**

It is a self-executing software that is currently developed in Go (identical to smart contracts).

**Channels:**

It is a confidential "subnet" of communication between specific network users (or hospitals), with the intention of facilitating private transactions.

**Ordering service:**

It guarantees the regularity and planning of transactions

**Endorsement policy:**

It consists of the set of guidelines that a node can use to determine whether or not a transaction is accepted.

**Application SDK**:

Based on the endorsement policy outlined in the chain codes, it approves transactions prior to commitment

**Endorsing peers:**

To validate the blocks, it obtains them from the ordering service.

**Committing peers:**

It also updates the state of the data in the State DB and the ledger.

**Disease diagnosis process:**

The VAE model, which correctly detects the presence of disease, is used to diagnose the condition from the medical records. Min—Max data normalisation is used to normalise the data before using the VAE model. The appropriate class labels for the applied health records are then determined using the VAE model. In the latent parameter space, the VAE network offers a probabilistic perception. Using the latent parameter z to define the sharing of the novel dataset is one of the VAE's key goals. They believe that the Gaussian distribution is necessary for the qualified sharing of the latent parameter z. Figure 5 depicts the VAE structure. This idea shows how the hidden parameter z satisfies the Gaussian distribution, which might be used by NN to produce information that satisfies some distribution. The latent parameter z provides a dataset that is comparable to the actual data by boosting the produced variable. It follows that it would take use of the marginal probability

Equation:14

The VAE presents an identifying component q(z|x) to estimate the uncertain true posterior p(z|x), as the true posterior density p(z|x) is intractable. By using Kullback-Leibler (K L) divergence, the VAE compares the identification module q(z|x) with the genuine posterior distribution p(z|x).

Equation:15

Since the KL divergence is generally greater than zero

This equation named (i.e., variational) low bound on peripheral probability of data point i, is stated as follows:

Equation:16

The variational lower bound on the marginal probability sets the entire optimization goal of VAE in order to improve logp(x). The initial term on the right side of Eq. (16) corresponds to the regularisation term and a negative autoencoder reconstruction error. As a result, p (x(i) | z) is referred to as a probabilistic decoder with generation variable, and q(z|x(i)) is referred to as a probabilistic encoder with variational variable and (). The Bernoulli/Gaussian distribution is frequently provided under the conditional distribution p (x(i) | z). Instead of binary data, patient medical records are used as the network's inputs in this study, and the distribution p (x(i) | z) is thought to be Gaussian. In a later step, they calculate the stochastic gradient variational Bayes estimator of the variational lower limit (,, x(i)). They use the reparameterization method to present the identification module q(z|x(i)), where z is a continuous arbitrary parameter and q(z|x(i)) is a conditional distribution with a summary of an auxiliary noise variable p(). In this case, the marginal probability distribution for p() is known. The result of applying a distribution conversion on the data in q(z|x(i)) is z g(, x(i)). They consider qφ(z|x(i) ) that fulfills a Gaussian distribution where (z) N(z; 0, I). The calculation qφ(z|x(i) ) N(z; u, σ2 I), regularization term is given by Equation:17

Figure 6

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

Equation18

The data reconstruction is predicated on the VAE principle, and the exception's fundamental cause is looked at. The entire module is learned throughout the module's training phase using standard medical records. As a result, the decoder and encoder of the module would show on the rebuilt data of the hidden parameter z if the modules achieved superior illness diagnostic results on the tested data. This section uses the Heart Statlog, Pima Indian Diabetes, and EEG Eye-state datasets to evaluate the performance of the proposed HBESDMDLD approach. 270 instances with 13 attributes make up the initial Heart Statlog dataset. There are 768 cases with 8 attributes in the second PIMA Indians diabetes dataset. Eventually, there are 14,980 cases with 15 attributes in the EEG Eyestate dataset. Table 2 provides the detailed dataset.

Table 3 and Fig. 6 provide a thorough security study of the GTOA-SIMON approach on three different datasets. It is evident from the table values that the GTOA-SIMON technique has For example, the GTOA-SIMON technique obtains an encryption time of 6.82 s, a decryption time of 6.70 s, and a security level of 93.28% on the cardiac statlog dataset with 20% data size. The GTOA-SIMON technique therefore achieves an encryption time of 31.88 s, a decryption time of 24.87 s, and a security level of 93.52% with 100% of the data size. Likewise, the GTOA-SIMON technique produced decryption and encryption times of 9.63 and 8.35 seconds, respectively, and a security level of 92.78% on the PIMA Indian diabetes dataset with 20% data size. The GTOA-SIMON technique therefore achieves an encryption time of 47.08 s, a decryption time of 44.01 s, and a security level of 95.87% with 100% of the data security in terms of encryption time, decryption time, and security level. Similarly, the GTOA-SIMON technique produced encryption and decryption times of 21.73 and 19.82 seconds, respectively, and a security level of 93.70% on the EEG EyeState dataset with 20% data size. The GTOA-SIMON technique thus achieves an encryption time of 95.38 s, a decryption time of 93.03 s, and a security level of 96.84% with 100% of the data amount.

A brief comparative analysis is presented in Table 4 and Fig. 7 to ensure the GTOA-SIMON technique's increased security efficiency. According to the results, the Blowfish approach has the lowest security rating (90.81%). The security levels for the ECC and RSA models, respectively, have increased somewhat and are now 91.03% and 91.67%. Concurrently, 94.29% and 93.71%, respectively, of reasonable security levels have been reached using the SIMON and SC techniques. Nonetheless, with a maximum security level of 94.46%, the GTOA-SIMON approach has achieved notable efficiency.

Table 5 and Fig. 8 provide a thorough comparison of the HBESDMDLD's results with those obtained using the Heart Statlog dataset [37, 38]. It is clear from the findings that the RT model has the least outcome and the lowest accuracy (0.76). Likewise, the J48 model has marginally improved performance, with an accuracy of 0.77.

Table4

Figure 7

Figure 8

Table 5

Next, the RBF Network model, with an accuracy of 0.84, predicted a mild outcome. The EEPSOC-ANN and GBT models both concurrently displayed respectable accuracy of 0.95 and 0.95, correspondingly. The provided HBESDMDLD strategy surpassed all other methods with a maximum accuracy of 0.98, despite the DOD-GBT model trying to achieve an optimal efficiency of 0.96.

Table 6 and Fig. 9 [39] provide a thorough comparison of the results obtained using the HBESDMDLD and currently used methods on the Pima Indian Diabetes dataset. It is clear from the data that the Voted Perceptron technique yields the least accurate results, with a minimal accuracy of 0.67. The DT model's performance has also been marginally improved, with an accuracy of 0.74. Next, the LogitBoost model, with an accuracy of 0.74, showed a moderate outcome. The LR model has simultaneously demonstrated a respectable accuracy of 0.77. The reported HBESDM-DLD technique surpassed all other strategies with a better accuracy of 0.95, despite the MR-OGBT model's attempts to achieve the ideal correctness of 0.89.

Table 7 and Fig. 10 show a thorough comparison of the HBESDMDLD's results with those of other methods on the EEG EyeState dataset [40, 41]. Findings indicate that the least productive RT model has the lowest accuracy of 0.76.

Table 6

Figure 9

Table 7

Figure 10

Meanwhile, SA-LSTM has greater performance with 0.86 of accuracy. Both the RS-LSTM and DE-LSTM approaches have simultaneously demonstrated a respectable and comparable accuracy of 0.90 each. With a maximum accuracy of 0.93, the reported HBESDM-DLD approach surpassed all other models.

The study of the results described above makes it clear that the HBESDM-DLD technique has achieved the maximum level of secrecy while having a considerable detection accuracy. As a result, it can be used in a real-time setting for the secure transmission of medical records and the associated diagnostic procedure.

**Conclusion**

A novel HBESDM-DLD model for secure data transfer and diagnostic procedures has been created in this research. The concept that is being described consists of many stages of activities, including SIMON block cipher-based encryption, GTOA-based optimum key generation, secure data management using the Hyperledger blockchain, and VAE-based diagnosis. The health record transmission procedure has increased security due to the inclusion of GTOA in the key generation process. The hyperledger blockchain, meanwhile, offers secure health record management, allowing patients to grant or revoke access to any doctor or healthcare facility. Finally, the VAE-based diagnostic procedure is used to identify any disorders that may occur. Using a benchmark medical dataset, the HBESDMDLD research's data are evaluated, and the findings are assessed using a variety of performance metrics. The experimental findings show that the HBESDM-DLD methodology outperforms cutting-edge techniques. Future versions of the HBESDM-DLD approach could incorporate training speed schedules for the VAE model and a hyperparameter optimizer based on metaheuristic optimization.