Journal of Theoretical and Applied Information Technology

15th September 2023. Vol.101. No 17
© 2023 Little Lion Scientific

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

HBESDM-DLD: A SECURE BLOCKCHAIN-BASED MEDICAL DATA MANAGEMENT WITH DEEP LEARNING-BASED DIAGNOSTIC MODEL

Mr. SUNIL KUMAR RM[1]*, Dr. A. JAYACHANDRAN[2]

[1] School of Computer Science Engineering, Assistant Professor, Presidency University, India

[2] School of Computer Science Engineering, Associate Professor, Presidency University, India

E-mail: [1] sunilcse4@gmail.com , [2] ajayachandran@presidencyuniversity.in

ABSTRACT

The healthcare sector has witnessed significant growth in electronic health records (EHRs) generation. While the EHR system provides data owners with control over their data and sharing permissions, the vast amount of healthcare data poses challenges in ensuring security and accurate diagnosis. This paper introduces the HBESDM-DLD model, a novel approach that employs blockchain technology and deep learning for secure medical data management and diagnosis the suggested paradigm contains steps for diagnostics, hyper ledger-based safe data management, optimal key generation, and encryption. Users can manage data access using the model permits hospital authorities to read and write data, and notifies emergency contacts. To enhance security, the elliptical curve cryptography technique is utilized for encryption, with the arithmetic optimization algorithm (AOA) applied for efficient key generation. Multi-channel hyper ledger blockchain is used for sharing medical data, storing patient visit data, and recording EHR links in external databases. Finally, the Spiking Neural Network (SNN)- Following data decryption, an evidence-based diagnostic approach is used to identify disorders. Medical benchmark datasets are used to assess the performance of the HBESDM-DLD model, and better performance than current techniques is shown.

Keywords: *Encrypted Health Record, Encryption, Unauthorized Access, Decryption, Medical Data Management, Optimal Solution*

1. INTRODUCTION

The healthcare industry is constantly generating large amounts of electronic data, from patient records to medical research findings [1] [2]. As such, there is a growing need to guarantee the security, privacy, and accessibility of this information. With the increasing prevalence of cyber threats, data breaches, and identity theft, traditional methods of securing sensitive information have proven insufficient [3][4]. To address these challenges, healthcare providers are exploring innovative technologies such as blockchain and smart contracts. Blockchain is a decentralized, distributed ledger that is maintained by a network of computers or nodes. It operates without a central authority, relying instead on a consensus mechanism to validate transactions. Each transaction is recorded on the blockchain and stored on every node in the network, creating an immutable and transparent record of all activities [5] [6] [7]. This transparency and security make it an ideal solution for managing electronic healthcare records (EHRs).

Using blockchain technology as a foundation, smart contracts are self-executing software applications. They can be used to automate the process of verifying, executing, and enforcing the terms of an agreement between parties [8]. Smart contracts eradicate the requirement for intermediaries, such as lawyers or other trusted third parties, thereby reducing costs and increasing efficiency. They can also be used to set conditions for accessing EHRs, such as granting or revoking access to specific individuals based on predefined rules Using smart contract technology together would enhance the security and usability of Ehr systems in a number of ways. Firstly, blockchain technology ensures that all data is stored in a tamper-proof manner [9] [10] [11] [12], making it difficult for malicious actors to alter or delete data. Secondly, smart contracts can automate the process of verifying user identity, granting or revoking access to data, and ensuring that data is accessed only by authorized personnel. This can help prevent data breaches caused by human error or negligence, such as accidentally sharing login credentials or forgetting to revoke access when an employee leaves the organization.

Moreover, blockchain technology can improve the interoperability of EHRs by allowing different providers to share information securely and efficiently [13] [14] [15]. The lack of interoperability has been a longstanding issue in the healthcare industry, hindering the delivery of quality care and research. By using a decentralized platform, healthcare providers can share data across different organizations while maintaining control over who has access to what information. This study examines how blockchain technology and smart contracts might be used to safeguard electronic health records in the healthcare sector. In this article, we look at the advantages and drawbacks of employing this technology propose a framework for implementing a blockchain-based system for managing EHRs. Our proposed framework includes a secure and decentralized storage system, patient-controlled access management, and a permissioned network for sharing EHRs between healthcare providers. The appropriation of Blockchain innovation in the healthcare sector can help to address the issues with EHRs and advance the standard of patient care. Security and privacy can be ensured by employing the blockchain and smart contracts of patient data while providing healthcare professionals with timely access to accurate patient records. This article adds to the expanding amount of literature on the use of blockchain technology in healthcare and provides insights into this technology's potential to completely change the healthcare sector. The organization of the remaining paper is as follows: Section 2 presents a review of the literature on existing methods for secure medical data management and diagnosis, Section 3 describes the distinct stages of operations involved in the HBESDM-DLD model, including “encryption, optimal key generation, hyper ledger-based secure data management, and diagnosis”. Section 4 examines the performance of the HBESDM-DLD model in comparison to other approaches and gives the experimental findings. The summary of the paper is presented in Section 5.

2. LITERATURE REVIEW

In the short term, efforts will be concentrated on creating a user-friendly website that leverages blockchain technology to safeguard all medical data collected from doctors and patients. Nevertheless, several academic publications have already investigated the effectiveness of blockchain in healthcare, and a few of the most vital research works are highlighted below.

Shahnaz, et al. 2019 [16] explored possibilities of cryptocurrency technology in transforming EHR systems as a potential solution to the issues related to their secure storage and access. The researchers proposed a plan for using blockchain technology inside the healthcare sector sector specifically for EHR, with the primary goal of providing secure storage of electronic records. This framework also addressed the issue of scalability that is typically faced by blockchain technology by incorporating off-chain storage of the records. With this proposed system, the EHR framework might have delighted in the advantages of a versatile, secure, and integral blockchain-based arrangement. The system also characterized granular contact instructions for the clients of the proposed framework to guarantee that patient privacy and information integrity were maintained.

Pandey and Litoriya, 2020 [17] explained how healthcare data plays a critical role in policymaking, patient care, and medical diagnostics, but it is also vulnerable to cyber-attacks due to its significance and market demand. They noted that centralized record-keeping systems in the healthcare sector create a single point of attack for hackers. To address this vulnerability, they proposed a decentralized system using blockchain technology, which employs robust cryptography methods. They described in their study a safe blockchain-based architecture that was suited to the needs for e-healthcare systems. The proposed architecture aimed to ensure patient data security and privacy while offering the advantages of decentralization and distribution.

Tanwar, et al. 2020 [18] investigated various approaches to tackle the limitations of healthcare systems by utilizing blockchain technology. The proposed solutions included different frameworks and tools, such as “Hyperledger Fabric, Hyperledger Composer, Docker Container, Hyperledger Caliper, and the Wireshark capture engine, that enabled measuring the performance of blockchain-based systems". Additionally, to improve data accessibility among healthcare professionals, an Access Control Policy Algorithm was proposed. The creation of an EHR sharing system built on the Hyperledger blockchain and using the chain code was also covered in the study. concept, which was simulated for performance evaluation. The study focused on optimizing the performance metrics of "blockchain networks, such as latency, throughput, and Round-Trip Time (RTT), to achieve improved results".

Nishi, et al. 2022 [19] proposed a cryptocurrency system that provides a secure and effective way to organize and save patient data into a single record under the patient's control. The Ethereum network was used to create the system with Solidity and web3.js programming languages and tools. The proposed approach used smart contracts to store and manage patients' data in a decentralized manner, ensuring security and privacy. The smart contract executed transactions that were verified and conveyed to the entire distributed network. Access to the system was provided through a cryptocurrency wallet (MetaMask) that ensured the documents' security and confidentiality. The proposed system offered benefits such as efficient data access and sharing, secure storage of data, and secure transfer of patient medical records. This system also enhanced credibility and reduced barriers by enabling users to access the same data at the same time. The proposed health-record system and protocol enabled greater transparency and ownership of sensitive data while promoting the healthcare sector with blockchain technology.

Chelladurai and Pandian, 2022 [20], proposed a system that used blockchain smart contracts to develop a safe and regulated healthcare solution for patients, doctors, and other healthcare professionals. The goal was to facilitate the "exchange of health information through a blockchain platform and establish a smart e-health system". The framework utilized an Altered Merkle Tree information structure to form a permanent patient log and guaranteed secure capacity and fast access to wellbeing records. The stage moreover empowered the "upgrade of therapeutic records, wellbeing data trade between distinctive suppliers, and viewership contracts on the peer-to-peer blockchain network". In this framework, the blockchain served as a clinical information store that supplied complete, distributed records to patients that included all their electronic well-being records. Security and keenness were guaranteed through cryptographic hash functions. The proposed system underwent multiple trials to evaluate its effectiveness, including qualitative and quantitative metrics to measure the "performance of resources, transactions per second, and transaction latency".

Mahajan, et al. 2022 [21] conducted a comprehensive investigation of "contemporary blockchain-based techniques for securing medical data, whether or not cloud computing" was involved. The paper explored a range of methods and evaluated their efficacy. The study yielded several outcomes, including identifying gaps in research, highlighting challenges, and outlining a future roadmap for advancing Healthcare 4.0 technology.

Kim, et al. 2020 [22] introduced a protected protocol for an electronic health record (EHR) system that was cloud-assisted and used blockchain technology. The proposed scheme aimed to enhance access control and data integrity via log transactions secure storage on a cloud server to determine how well the elliptic cryptosystem (ECC) works with cloud computing for safe health data sharing, a study was done. The suggested electronic medical record (EHR) system has been assessed in accordance with "informal security analysis and automated validation of internet security protocols and applications (AVISPA) simulation to ensure its security". In addition, the paper compared the proposed system's security characteristics and its communication and computation overheads with existing schemes to demonstrate its efficiency and effectiveness. The proposed EHR system provided secure and efficient solutions for practical healthcare systems.

Zarour, et al. 2020 [23] employed a systematic approach to assessing the effect of different blockchain model implementations on healthcare administration, offering fresh insight for future academics. 56 healthcare management domain specialists worked to do this were surveyed to assess the influence of various blockchain models. To address the issue of multiple opinions, a decision model was used to externalize and assemble data about the blockchain model's context of choice. The research made use of "Fuzzy Analytic Network Process (F-ANP) method to calculate the criteria weights, and the Fuzzy-Technique for Order of Preference by Similarity to Ideal Solution

(TOPSIS) technique was employed to assess the impact of alternative solutions”. By doing so, the study was able to reduce ambiguities and provided a more objective analysis of bitcoin technology's effects on healthcare management.

Shen, et al. 2019 [24] introduced to increase the effectiveness of sharing, a new healthcare data-sharing programme called MedChain was created both structured and unstructured healthcare data. MedChain employed a combination of “blockchain, digest chain, and structured P2P network techniques” to address the limitations of existing data-sharing approaches. The proposed scheme also offered session-based data sharing, which allowed for greater flexibility in data sharing.

Nagasubramanian, et al. 2020 [25] A cloud-based system was proposed that provides authentication and integrity to health records. The proposed system used keyless signature infrastructure for digital signature secrecy and authentication and blockchain technology for data integrity. The average duration, size, and expense of storing and retrieving information were used to gauge the proposed study's validity compared to conventional storage techniques.

2.1 Research Gap

As a viable remedy to address the problems associated to the healthcare industry, the usage of blockchain technology has been secure storage and access of EHRs [26] [27]. The current centralized record-keeping systems used in the healthcare sector expose a single node for attackers to exploit, making them vulnerable to cyber-attacks. Blockchain technology provides a decentralized and distributed system that uses reliable cryptographic algorithms to secure patient data. The use of blockchain technology in healthcare, however, is fraught with difficulties, such as scalability and performance metrics [28]. Several studies have proposed frameworks, tools, and algorithms to improve the current limitations of healthcare systems using blockchain technology. Moreover, studies have examined several using and not using the cloud, blockchain-based methods for preserving medical data. Secure archiving, quick access, and interchange of health records are the objectives of the suggested solutions. between different healthcare providers, ensuring patient privacy and data integrity.

3. PROPOSED METHODOLOGY

3.1 The proposed HBESDM-DLD model

The HBESDM-DLD model is a comprehensive system for managing and securing patient health records. It involves several stages of operations, including “encryption, optimal key generation, hyper ledger blockchain-based secure data management, and diagnosis”. To begin with, the patient's health records are encrypted by employing the Elliptic Curve Cryptography (ECC) method, which is renowned for its high security and compact key size. The AOA-based optimal key generation technique is used to generate a unique and secure key for the encryption process. The Hyperledger blockchain is then utilized to store the encrypted health records securely. The blockchain consists of a global blockchain and several local blockchains for medical institutions, ensuring that patient data is accessible only to authorized parties. The patient has complete control over who can access their health records, and they can permit or revoke access to physicians or medical organizations at any time. When an authorized user requests access to the patient's health records, the encrypted data can be decrypted by the authorized user using the optimal key generated during the encryption process. This allows them to retrieve the actual health records and perform necessary diagnoses. Finally, the Spiking Neural Network (SNN)- employing the ECC method, renowned for its high security and compact key size or conditions. By using this model, patient health records can be securely managed, and sensitive information can be protected from unauthorized access.

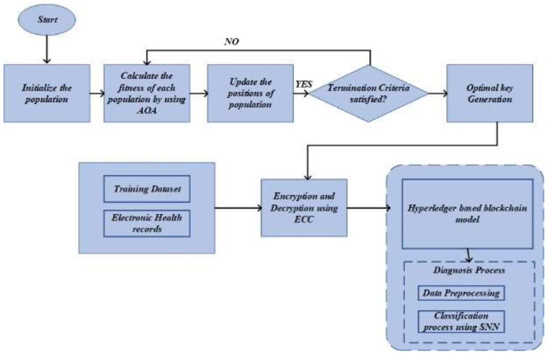

Start
NO
Initialize the population
Calculate the fitness of each population by using AOA
Update the positions of population
YES
Termination Criteria satisfied?
Optimal key Generation
Training Dataset
Electronic Health records
Encryption and Decryption using ECC
Hyperledger based blockchain model
Diagnosis Process
Data Preprocessing
Classification process using SNN

Figure 1: Block diagram of HBESDM-DLD model

3.2 DATA ENCRYPTION PROCESS USING ECC

ECC utilises a pair of public and private keys for encryption / decryption. Alice and Bob are two parties who wish to communicate securely. They must first agree on an elliptic curve equation and a generator point G. Each party generates a private key: nA for Alice and nB for Bob. These private keys are kept secret. The public keys are then derived by multiplying the generator point G_r with the respective private keys: Alice's public key is $nA * G_r$ and Bob's public key is $nB * G_r$ which is stated in Eq. (1) and (2). The public keys of Alice and Bob are specified by

$$P_a = nAG_r \tag{1}$$

and

$$P_b = nBG_r \tag{2}$$

respectively. If Alice wants to send Bob a message 'P_m,' she encrypts it with Bob's public key. Eq. (3) states the cipher text which is given by

$$P_c = \{kG_r, P_m + kP_b\} \tag{3}$$

where 'k' denotes a random integer. The random 'k' ensures that even though the message is the same, the cypher text created is unique each time. This makes it difficult for anyone attempting to decrypt the message illegally. Bob decrypts the message by subtracting the '$P_m + kP_b$'from 'kG_r' ' multiplied by nB which is denoted in Eq. (4).

$$P_m = \{P_m + kP_b - nBkG_r\} \tag{4}$$

Multiplied here does not refer to basic multiplication as in mathematics, but rather to multiple additions of points using the point addition method described above under point multiplication. Because the multiplier nB is Bob's secret key, only Bob can decrypt Alice's message.

3.2.1 HBESDM-DLD algorithm

Algorithm 1: ECC addition and HBESDM-DLD secure medical data management

```
Input: EHR reading for patient P1
Output: Add blocks to the patient P1 blockchain and patient P1 HBESDM-DLD
Step 1: EHR←Patient P1 and read EHR
Step 2: Public Key and Private Key←key generation using ECC
Step 3: For encryption patient p1←Public key
Step 4: Doctor ← Shared the private key and Insurance Agency for Decryption purposes
Step 5: Encrypted HER ← Encrypt EHR Public key-based ECC
Step 6: ECC ← Hash key for EHR encryption based on AOA
Step 7: SNN ← Create a disease diagnosis process for Patient P1 with EHR encryption.
Step 8: Use the patient's user ID, password, and patient code to create a hyper ledger block for the Patient P1 blockchain.
Step 9: Block← Put the hash key value and SNN encryption for EHRs.
Step 10: HBESDM-DLD-based secure block to Patient P1 blockchain
Step 11: Stop
```

3.3 OPTIMAL KEY GENERATION PROCESS USING AOA

Population-based algorithms typically start by generating a set of candidate solutions at random, which are then improved through a series of optimization rules and evaluated using an objective function. The goal of these to identify the best solution stochastically, use algorithms to an optimization problem, but a single run may not necessarily yield a solution. The possibility of finding the overall ideal solution rises by producing one can generate a sufficient number of random answers and then carry out multiple optimization iterations to improve the results. While there are differences between various meta-heuristic algorithms that utilize population-based optimization methods, they generally consist of two main phases: exploration and exploitation. "Exploration involves searching the search space extensively using search agents to avoid local solutions, while exploitation involves improving the accuracy of solutions obtained during the exploration phase". The proposed AOA algorithm utilizes Arithmetic operators, specifically Multiplication, Division, Subtraction, and Addition, to achieve exploitation (intensification) and both diversification and exploration strategies. Figure 1 shows how these mechanisms operate. AOA is a meta-heuristic algorithm with a population-based design that can solve optimization problems without the need to calculate their derivatives.

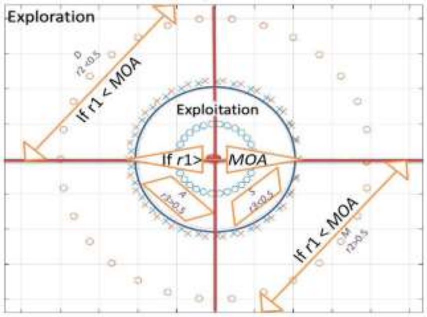


Figure 2: Phases of the AOA

The suggested AOA approach is motivated by the usage of arithmetic operators to tackle arithmetic problems. The behaviour of the arithmetic operators, "Multiplication (M), Division (D), Subtraction (S), and Addition (A), and their effects on the algorithm," are covered in the following subsections. Arithmetic operators in order of complexity is depicted in Figure 2 with increasing dominance from the outermost level to the innermost level.(

Step 1: Initialization phase

The optimization process in AOA commences with a group of possible solutions (X) represented by Matrix (5). These solutions are generated at random, and in each iteration, the most exceptional candidate solution is regarded as the best-obtained solution, or as an approximation to the optimal solution obtained so far.

$$X=\begin{bmatrix} x_{1,1} & \cdots & \cdots & x_{l,m} & x_{1,n-1} & x_{1,n} \\ x_{1,2} & \cdots & \cdots & x_{2,m} & \cdots & x_{2,n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{N-1,1} & \cdots & \cdots & x_{N-1,m} & \cdots & x_{N-1,n} \\ x_{N,1} & \cdots & \cdots & x_{N,m} & x_{N,n-1} & x_{N,n} \end{bmatrix} \qquad (5)$$

Before commencing the optimization process with AOA, the search phase must be determined - either investigation or exploitation. It is possible to calculate a coefficient using the Math Optimizer Accelerated (MOA) function. by Eq. (6), and it is employed in the search phases that follow.

$$MOA(CN_{Iter}) = Min + CN_{Iter} \times \left(\frac{Max - Min}{M_{Iter}}\right) \qquad (6)$$

The value of MOA at the tth iteration is represented by MOA(CNIter) and is obtained by evaluating Eq. (6). CNIter corresponds to the current iteration number, which ranges from 1 to the maximum number of iterations (MNIter). The accelerated function's minimum and maximum values are denoted by the variables Min and Max, respectively.

Step 2: Exploration phase

During the AOA's exploration stage, the exact location is erratically discovered across multiple regions, to discover a better answer. There are two main search methods used in this phase – "the Division (D) search strategy and the Multiplication (M) search strategy" - both of which are demonstrated in Eq. (7). The MOA function, as described in Eq. (6), conditions this search phase. Specifically, the exploration phase is

$$x_{l,m}(CN_{Iter}+1)=\begin{cases} best(x_m)\div(MOP+\epsilon)\times((UB_m-LB_m)\times\mu+LB_m)), & f2<0.5 \\ best(x_m)\times MOP\times((UB_m-LB_m)\times\mu+LB_m)), & otherwise \end{cases}$$

initiated when a randomly generated number, f1, exceeds the value of MOA. The first operator (D), which is the initial rule in Eq. (7), is triggered when the value of F2, a further created number, is less than 0.5. The second operator (M) is now momentarily disregarded. On the other hand, if the second operator (M) is necessary to complete the current task, D is discontinued, and M takes over. This decision is based on the value of another randomly generated number, f2.
(7)

In Eq. (8), xl (CNIter+1) refers to the lth solution in the next iteration, while xl,m (CNIter+1) indicates the mth position of the lth solution in the current iteration. The mth position in the best-obtained solution so far is represented by best (xm). "The value of ϵ is a small integer, and UBm and LBm signify the upper and lower bounds of the mth position, respectively". Additionally, μ is a control parameter used to regulate the search process and is set to a fixed value of 0.5 based on the experiments conducted in this study.

$$MOP(CN_{Iter}) = 1 - CN_{Iter}\frac{1}{\alpha}MN_{Iter}\frac{1}{\alpha} \qquad (8)$$

The function value at the tth iteration is represented by MOP(CNIter) in Eq. (8), where MOP is a coefficient determined by the Math Optimizer probability. The parameter α is a sensitive variable that governs the level of exploitation accuracy across iterations and is set to a fixed value of 5 based on the experiments conducted in this study.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Step 3: Exploitation phase

The exploitation strategy of AOA is outlined in this section. Based on the Arithmetic operators, using "either Subtraction (S) or Addition (A) in mathematical calculations can produce high-density results, indicating an exploitation search mechanism". As demonstrated in Figure 3, S and A have lower dispersion than other operators, making it simpler for them to approach the target. Therefore, the exploration study reveals a nearly ideal resolution that is possible after repetitions. During the optimization process, the exploitation operators (S and A) were utilized to improve communication between them and support the exploitation stage. The exploitation search phase, which involves executing S or A, is dependent on the MOA function value. More precisely, it is specified by the condition that f1 is not greater than the current value of MOA (CNiter) (as shown in equation (6)). In AOA, "the mining operators (subtraction (S) and addition (A)) explore the depth-first search over some dense regions and use two main search strategies (i.e., the search strategy). Search for subtraction (S) and search strategy for addition (A))", shown in equation (9).

$$x_{l,m}(CN_{Iter}+1)=\begin{cases} best(x_m)-MOP\times((UB_m-LB_m)\times\mu+LB_m), & f3<0.5 \\ best(x_m)\times MOP\times\left((UB_m-LB_m)\times\mu+LB_m\right), & otherwise \end{cases} \quad (9)$$

During this phase, the goal is to thoroughly explore the search space, as illustrated in Figure 3. The first operator, S, is applied under the condition that f3 < 0.5. Only when S has finished its current task is the second operator, A, invoked. S will assume the lead if A is unable to finish the job. Similar to the partitioning employed in the prior phase, the exploitation operators (S and A) are attempting to avoid becoming ensnared in local search areas in this procedure.

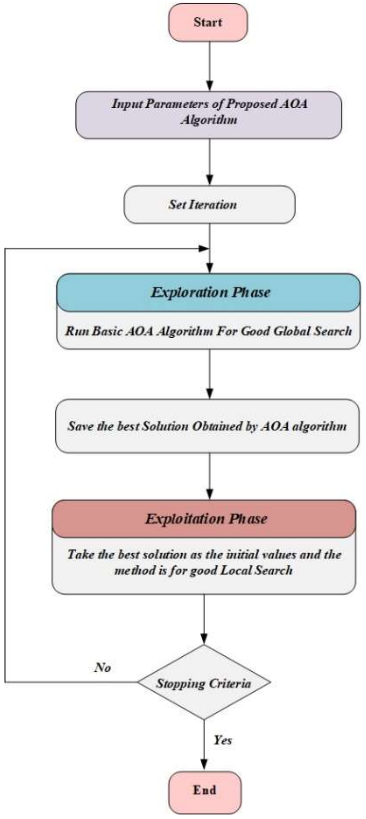

Start
Input Parameters of Proposed AOA Algorithm
Set Iteration
Exploration Phase
Run Basic AOA Algorithm For Good Global Search
Save the best Solution Obtained by AOA algorithm
Exploitation Phase
Take the best solution as the initial values and the method is for good Local Search
No
Stopping Criteria
Yes
End

Figure 3: Flowchart of AOA

3.4 HYPERLEDGER BLOCKCHAIN

The application of federated learning in this research combination with a machine learning-based disease diagnostic model is explored within the context of blockchain technology. A shared ledger technology called cryptocurrency offers advantages such as "availability, suitability, privacy, integrity, and decentralization". Decentralization ensures that data stored on the blockchain is replicated over several computers, removing the possibility of a single point of failure. Availability allows for access to the data even in the event of some computer failures. Integrity ensures that data is protected from inappropriate modifications, while suitability allows for the tracing of all data stored on the blockchain. Privacy enables members to remain anonymous. From a technical perspective, the blockchain is made up of a series of interconnected and trustworthy blocks, each containing a header and data. The header incorporates different components such as a "signature, identifier, and the previous block". A universally unique value developed by a scientific study and associated with each block of data may serve as the identifier. In square chaining, the previous block is in charge of ensuring that the identification value of each unused piece included in the chain matches to the prior block, creating a coherent chain of links.

Some open-source blockchains are powered by the Blockchains management platform, including super ledger structures. Its purpose is to provide a decentralized environment, with components such as "endorser peer, order, certificate authority, client, and committing peer". These components are connected using channels that enable transactions to be carried out privately and securely, while also splitting different application domains. The fabric certificate authority has two main responsibilities: first, to ensure that various components can use the system as intended, and second, to validate and authorize components to carry out certain functions or access other components. The committing peer must store the chain sent on the system-created channel. It stores a different blockchain for every individual channel created. Having a separate chain for each channel provides scalability and privacy.

For privacy considerations, a component cannot access the chain from committed peers associated with a channel unless it has access to that network. In terms of scalability, by having a separate channel for each transaction, different transactions and data stored in different commit nodes can be shared, which increases the amount requested by the node and thus improves the scalability of the system. Authorizing peers are accountable for two measures: first, gathering transactions from clients, and second, analyzing them using the smart contract system to ensure that the transactions follow the relevant rules. Gathering peers also execute two procedures, namely obtaining customer transactions and arranging them to monitor the blockchain's reliability. So, on a given chain, all ordering peers must make sure that the transaction is transferred to the committing peer. This blockchain is useful for storing electronic health records (EHRs) relevant to a person. Instead of having multiple visits to the same medical institution, the blockchain saves a single visit. Each medical institution has its blockchain (referred to as a local blockchain) to store the relevant EHRs for the person. To set up the blockchain, the medical institution keeps only the necessary structure to perform the Hyperledger network.

Hyperledger Fabric implements network-consistent business logic using smart contracts known as chain code applications. The state resulting from a chain code is private and inaccessible to other chain codes unless authorized. There are two types of chain code to consider: "system chain code, which handles system-related transactions like policy configuration and lifecycle management, and application chain code, which keeps application states like digital assets or arbitrary data entries on the ledger". Chain code packages include metadata such as "the counterparty's name, version, and signature to ensure the integrity of the code and metadata". The program is installed automatically on the other party's local computer when the package is loaded to that party's network node. Enrollment functions are performed within smart contracts (chain code) for private healthcare institutions authorized by Fabric network administrators to manage and govern the network. Health authorities secure private networks with permissions for registered stakeholders to access via virtual private network connections (VPNs) for added security. During registration, patients provide information such as "name, social security number, address, and contact information". All parties, including the "main physician, hospital, laboratory, pharmacy, researcher, and insurance, register with the regulating healthcare authority". After verification, the public health authority provides a chain code address, and all parties can complete transactions on the network.

The healthcare sector's process in the hyper-ledger blockchain is illustrated in Figure 4. Hyperledger Fabric is a design strategy that is modular provides "security, resilience, flexibility, and scalability". It can incorporate various elements and adjust to the complexities and intricacies of the financial ecosystem. According to the block diagram, the main elements of the fabric technology include:

- Chain codes: Written in the Go language, they are self-executing programs like smart contracts.
- Channels: They are private subnets of communication among specific members or hospitals in the network to ensure confidential transactions.
- Ordering service: It guarantees the consistency and planning of transactions.

- Endorsement policy: It could be a set of guidelines that determine in case the exchanges are affirmed or not.
- Application SDK: This computer program advancement unit permits peers to communicate inside the network.
- Endorsing peers: They receive blocks from the ordering service for the aim of verifying and modifying the ledger's and the state website's status of the data.
- Committing peers: They get a few streets away from the ordering service, information in the State DB and the record's status can be approved and updated.

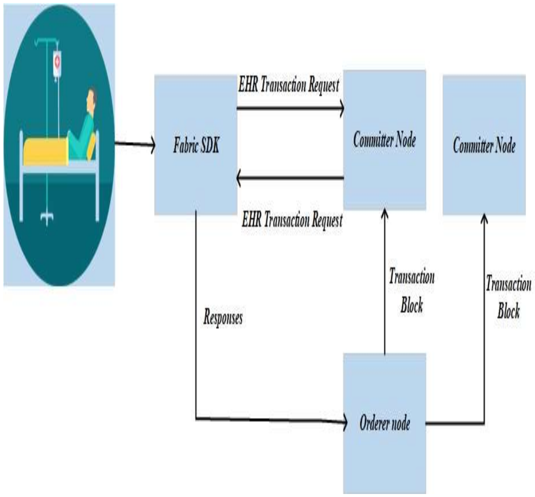


Figure 4: Flowchart of Hyperledger blockchain

3.5 DISEASE DIAGNOSIS USING SNN

The Spiking Neural Network (SNN) architecture is a model for a deep neural network that processes information in a way that resembles the behavior of biological neurons. In this approach, synaptic and neuronal states are temporally measured and evaluated for each neuron. SNNs do not fire every neuron instantaneously like conventional neural networks, which improves the network's quality. A neuron's activation produces circumstances that can raise or lower the neural threshold in the area. A cell that is more advanced may have an impact on the adjacent neurons' potential firing rates. The activity of the neuron stops if a threshold is not exceeded within a predetermined amount of time. The calculation of its value is based on the separation between neighboring impulses, and the firing of a neuron over time is depicted as an abruptly rising line. The Spiking network structure performs the use of coder and decoder techniques for the calculation of these values in numbers.

In the spiking model, each neuron considers all signals passed to it but does not fire immediately. It is necessary to fix the set trigger threshold so that the neuron's signal can be processed. The coding method used by the outlier model supports the upstream or downstream output that a neuron provides when it generates a threshold. The signal's pulse frequency and pulse range are both taken into account by this model. The decoder then translates each code into a sequence of numbers. The momentum values of spiking networks are computed using the Leakage Integral and Fire algorithm (LIF). The mathematical formula for the LIF algorithm takes into account the “current unit (I), the volt unit (V), the capacitor unit (C), the resistor unit (R), and the time unit (t)”. Figure 5 illustrates a sample graph of the temporal presentation of neurons over the threshold in a spiking network.

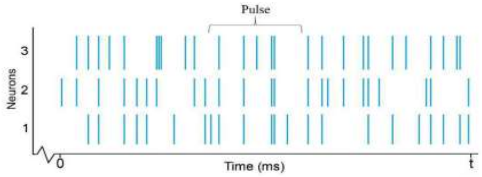


Figure 5: Temporal spike of neurons in spiking networks

$$I(t) - \frac{V_m(t)}{R_m} = C_m \partial \frac{V_m(t)}{\partial t}$$

Artificial neural networks (ANNs) and spiking networks both feature complicated network architectures but they differ in that they do not produce continuous output, as each neuron's output is determined by a threshold value. In Spiking networks when each neuron communicates with its neighbors, learning is facilitated. However, the cost of simulating the output in Spiking networks is higher than in the ANN model due to the use of specialized software such as “NEST, Brian, BindsNet, and GENESIS”. Spiking neural networks have a deep design consisting of an output layer, hidden layers, and an input layer which is exemplified in Figure 6.

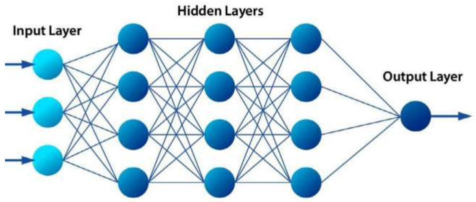


Figure 6: Layers of spiking networks

4. RESULTS AND DISCUSSION

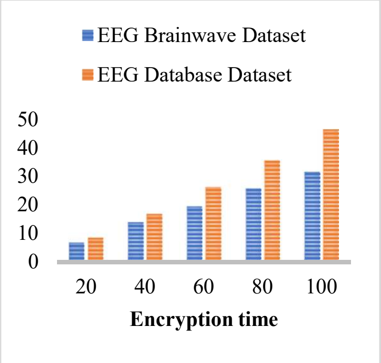
Two medical datasets, the EEG Brainwave Dataset, and the EEG Database Dataset were utilized to validate the efficacy of the HBESDMDLD technique. The EEG Brainwave Dataset and the EEG Database Dataset are two different datasets that contain information about EEG signals. “The EEG Brainwave Dataset contains 310 instances with 15 attributes, while the EEG Database Dataset contains 785 instances with 11 attributes. Both datasets have two classes, with class 1 containing 165 samples in the EEG Brainwave Dataset and 280 samples in the EEG Database Dataset. Class 2 contains 145 samples in the EEG Brainwave Dataset and 505 samples in the EEG Database Dataset.” EEG signals are electrical signals that are generated by the activity of neurons in the brain. They are used in a variety of applications, including medical diagnosis, cognitive neuroscience, and brain-computer interfaces. The datasets provide researchers with a valuable resource for exploring and analyzing EEG signals. The number of attributes in each dataset reflects the different types of information that can be obtained from EEG signals. The EEG Brainwave Dataset contains 15 attributes, which include alpha, beta, gamma, and delta brainwaves. The EEG Database Dataset, on the other hand, contains 11 attributes, which include the EEG signal amplitude and frequency.

Table 1 and figure 7 show the encryption and decryption times for two different datasets with varying data sizes and their corresponding security levels. EEG Brainwave Dataset has a security level ranging from 94.06% to 95.20%, while EEG Database Dataset has a higher security level ranging from 93.45% to 96.50%. As expected, the encryption and decryption times increase with the increase in data size for both datasets.

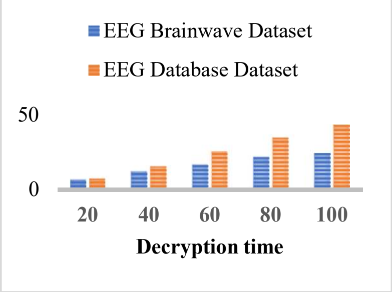
Table 1: Proposed AOA-ECC analysis

Data size (percent)	Encryption time (seconds)	Decryption time (seconds)	Security Level (percent)
EEG Brainwave Dataset			
20	06.75	06.58	94.06
40	14.01	12.27	94.21
60	19.55	16.70	95.18
80	25.83	21.96	95.20
100	31.69	24.74	94.09
EEG Database Dataset			
20	08.52	07.46	93.45
40	16.88	15.69	95.12
60	26.24	25.52	94.23
80	35.71	34.75	95.41
100	46.67	43.43	96.50

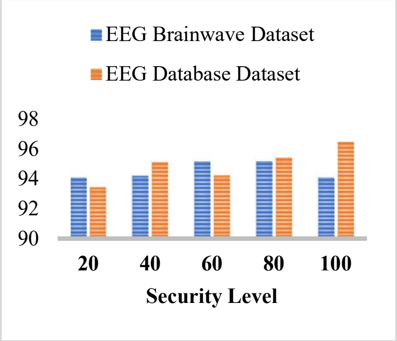
For EEG Brainwave Dataset, the encryption time ranges from 6.75% for a data size of 20% to 31.69% for a data size of 100%. The decryption time ranges from 6.58% for a data size of 20% to 24.74% for a data size of 100%. The highest security level is achieved for a data size of 80%, with an encryption time of 25.83% and a decryption time of 21.96%. For EEG Database Dataset, the encryption time ranges from 8.52% for a data size of 20% to 46.67% for a data size of 100%. The decryption time ranges from 7.46% for a data size of 20% to 43.43% for a data size of 100%. The highest security level is achieved for a data size of 100%, with an encryption time of 46.67% and a decryption time of 43.43%. Overall, EEG Database Dataset when compared to, offers a greater level of security EEG Brainwave Dataset, and also requires a longer encryption and decryption time.



(a) Encryption Time



(b) Decryption Time



(c) Security Level

Figure 7: Results of the proposed AOA-ECC model

Table 2: Comparative analysis between AOA-ECC-based and other security levels (%)

Methods	Security level
AOA-ECC	94.75
ECC	91.18
RSA	92.01
Blowfish	91.05

Table 2 and figure 8 provide a comparative analysis of various encryption techniques concerning the security level provided by AOA-ECC. The security level is expressed as a percentage, where AOA-ECC provides the highest security level at 94.75%. ECC, RSA, and Blowfish are the other encryption techniques compared in the table. ECC provides a security level of 91.18%, which is lower than AOA-ECC. RSA provides a security level of 92.01%, which is also lower than AOA-ECC. Blowfish provides a security level of 91.05%, which is the lowest among all the techniques compared in the table. The security level provided by an encryption technique is a crucial factor to consider when selecting a suitable encryption method for data protection. A higher security level implies a lower probability of unauthorized access and decryption data that has been encrypted. As a result, depending on the outcomes of this comparative analysis, AOA-ECC emerges as the most secure encryption technique.

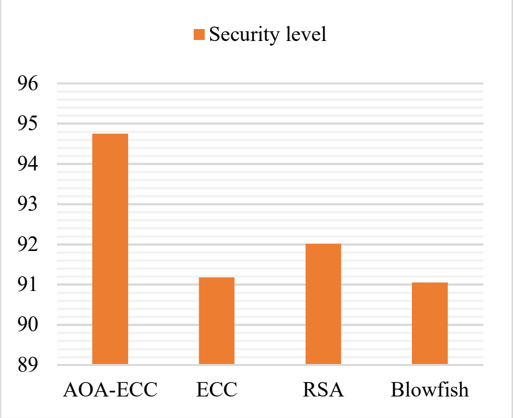


Figure 8: Security level analysis of the AOA-ECC model

Table 3: Performance comparison using EEG Brainwave Dataset (%)

Methods	Precision	Recall	Accuracy	F-Score
Proposed HBESDMDLD	97.54	98.22	98.41	98.06
RNN	96.28	97.95	96.67	96.34
DNN	96.71	94.88	95.59	95.47
SVM	73.55	74.18	77.39	75.06
Random Forest	75.12	73.77	77.26	74.58

Table 3 and figure 9 present the EEG Brainwave Dataset performance evaluation of the suggested and current HBESDMDLD method based on “Precision, Recall, Accuracy, and F-Score”. The proposed HBESDMDLD method outperforms all other methods with the highest scores across all the evaluation metrics. The precision score part of the suggested approach 97.54%, which is higher than RNN, DNN, SVM, and Random Forest. The recall the proposed method has the highest score of 98.22% out of all those compared in the table. The proposed approach has a score of accuracy of 98.41%, which is also the highest compared to other methods. Finally, the F-score of the proposed method is 98.06%, which is again the highest compared to other methods. RNN, DNN, SVM, and Random Forest are the existing methods compared in the table. Although RNN and DNN perform reasonably well, they still fall behind the proposed HBESDMDLD method. SVM and Random Forest, on the other hand, exhibit lower performance scores, especially in terms of clarity & recall. Overall, the results of this performance evaluation suggest that the proposed HBESDMDLD method is highly effective for EEG Brainwave Dataset classification, and it can provide superior accuracy and reliability compared to other existing methods.

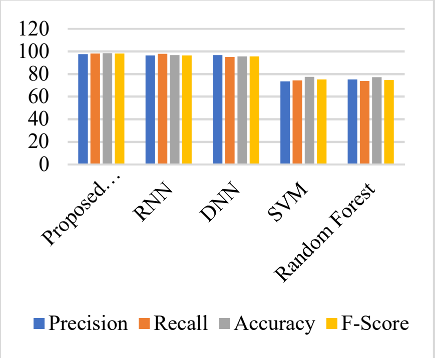


Figure 9: Comparative analysis on EEG Brainwave Dataset (%)

Table 4: Performance comparison using EEG Database Dataset (%)

Methods	Precision	Recall	Accuracy	F-Score
Proposed HBESDMDLD	94.89	96.88	95.74	94.51
RNN	92.12	92.56	90.18	92.79
DNN	84.81	79.22	75.45	82.64
SVM	93.71	69.15	68.21	78.33
Random Forest	89.48	78	77.45	83.82

Table 4 and figure 10 show the evaluation of the proposed and existing HBESDMDLD methods' performance using the EEG Database Dataset's Precision, Recall, Accuracy, and F-Score. In this case, the proposed HBESDMDLD method still performs better than all other methods. The precision score of the proposed method is 94.89%, which is the highest among all the methods compared in the table. The recall score of the proposed method is 96.88%, which is again the highest compared to other methods. The accuracy score of the proposed method is 95.74%, which is also higher than all other methods except RNN. Finally, the F-score of the proposed method is 94.51%, which is the highest compared to other methods. RNN performs reasonably well in this case, exhibiting the highest accuracy score of 90.18%. However, the precision and recall scores of RNN are lower than those of the proposed HBESDMDLD method. DNN, SVM, and Random Forest exhibit lower performance scores, in particular with regard to recall and precision. Overall, the results of this performance evaluation suggest that the proposed HBESDMDLD method can provide high accuracy and reliability for EEG Database Dataset classification, outperforming other in terms of accuracy, recall, and F-score compared to previous approaches.

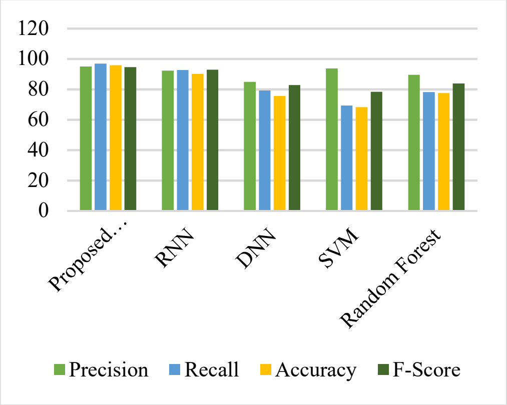


Figure 10: Comparative analysis of EEG Database Dataset

5. CONCLUSION

In conclusion, the proposed HBESDM-DLD model represents a promising approach for secure medical data management and diagnosis, leveraging the benefits of both blockchain and deep learning technologies. The comparative analysis of various encryption techniques with the proposed technique indicates that AOA-ECC is the most secure encryption technique, providing the highest security level of 94.75%. Therefore, it is recommended to use AOA-ECC for data protection when a high level of security is required. Similarly, The EEG Brainwave Dataset and EEG Database Dataset performance evaluation of the existing and proposed HBESDMDLD methods shows that the proposed method exceeds all other existing methods in terms of precision, recall, accuracy, and F-score. These findings imply that the suggested HBESDM-DLD approach can be highly effective for EEG dataset classification, providing superior accuracy and reliability compared to other existing methods. Overall, these findings can be useful for researchers and practitioners in the field of data security and EEG data analysis, as they can make informed decisions regarding the selection of suitable encryption techniques and classification methods based on their specific requirements and objectives.

REFERENCES:

[1] Sanchez-Pinto, L.N., Luo, Y. and Churpek, M.M., 2018. Big data and data science in critical care. *Chest*, *154*(5), pp.1239-1248.

[2] Dash, S., Shakyawar, S.K., Sharma, M. and Kaushik, S., 2019. Big data in healthcare: management, analysis and future prospects. *Journal of Big Data*, *6*(1), pp.1-25.

[3] Hughes-Lartey, K., Li, M., Botchey, F.E. and Qin, Z., 2021. Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*, *7*(3), p.e06522.

[4] Porcedda, M.G., 2018. Patching the patchwork: appraising the EU regulatory framework on cyber security breaches. *Computer law & security review*, *34*(5), pp.1077-1098.

[5] Niranjanamurthy, M., Nithya, B.N. and Jagannatha, S.J.C.C., 2019. Analysis of Blockchain technology: pros, cons and SWOT. *Cluster Computing*, *22*, pp.14743-14757.

[6] Helo, P. and Hao, Y., 2019. Blockchains in operations and supply chains: A model and reference implementation. *Computers & Industrial Engineering*, *136*, pp.242-251.

[7] Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C. and Santamaria, V., 2018. To blockchain or not to blockchain: That is the question. *It Professional*, *20*(2), pp.62-74.

[8] Hamilton, M., 2020. Blockchain distributed ledger technology: An introduction and focus on smart contracts. *Journal of Corporate Accounting & Finance*, *31*(2), pp.7-12.

[9] Unsworth, R., 2019. Smart contract this! An assessment of the contractual landscape and the Herculean challenges it currently presents for “Self-executing” contracts. *Legal Tech, Smart Contracts and Blockchain*, pp.17-61.

[10] Iftekhar, A., Cui, X., Hassan, M. and Afzal, W., 2020. Application of blockchain and Internet of Things to ensure tamper-proof data availability for food safety. *Journal of Food Quality*, *2020*, pp.1-14.

[11] Shekhtman, L. and Waisbard, E., 2021. Engravechain: A blockchain-based tamper-proof distributed log system. *Future Internet*, *13*(6), p.143.

[12] Javed, M.U., Javaid, N., Aldegheishem, A., Alrajeh, N., Tahir, M. and Ramzan, M., 2020. Scheduling charging of electric vehicles in a secured manner by emphasizing cost minimization using blockchain technology and IPFS. *Sustainability*, *12*(12), p.5151.

[13] Dagher, G.G., Mohler, J., Milojkovic, M. and Marella, P.B., 2018. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable cities and society*, *39*, pp.283-297.

[14] Kamau, G., Boore, C., Maina, E. and Njenga, S., 2018, May. Blockchain technology: Is this the solution to emr interoperability and security issues in developing countries?. In *2018 IST-Africa Week Conference (IST-Africa)* (pp. Page-1). IEEE.

[15] Gordon, W.J. and Catalini, C., 2018. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. *Computational and structural biotechnology journal*, *16*, pp.224-230.

[16] Shahnaz, A., Qamar, U. and Khalid, A., 2019. Using blockchain for electronic health records. *IEEE access*, *7*, pp.147782-147795.

[17] Pandey, P. and Litoriya, R., 2020. Securing and authenticating healthcare records through blockchain technology. *Cryptologia*, *44*(4), pp.341-356.

[18] Tanwar, S., Parekh, K. and Evans, R., 2020. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, *50*, p.102407.

[19] Nishi, F.K., Shams-E-Mofiz, M., Khan, M.M., Alsufyani, A., Bourouis, S., Gupta, P. and Saini, D.K., 2022. Electronic healthcare data record security using blockchain and smart

contract. *Journal of Sensors*, *2022*, pp.1-22.

[20] Chelladurai, U. and Pandian, S., 2022. A novel blockchain based electronic health record automation system for healthcare. *Journal of Ambient Intelligence and Humanized Computing*, pp.1-11.

[21] Mahajan, H.B., Rashid, A.S., Junnarkar, A.A., Uke, N., Deshpande, S.D., Futane, P.R., Alkhayyat, A. and Alhayani, B., 2022. Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems. *Applied Nanoscience*, pp.1-14.

[22] Kim, M., Yu, S., Lee, J., Park, Y. and Park, Y., 2020. Design of secure protocol for cloud-assisted electronic health record system using blockchain. *Sensors*, *20*(10), p.2913.

[23] Zarour, M., Ansari, M.T.J., Alenezi, M., Sarkar, A.K., Faizan, M., Agrawal, A., Kumar, R. and Khan, R.A., 2020. Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records. *IEEE Access*, *8*, pp.157959-157973.

[24] Shen, B., Guo, J. and Yang, Y., 2019. MedChain: Efficient healthcare data sharing via blockchain. *Applied sciences*, *9*(6), p.1207.

[25] Nagasubramanian, G., Sakthivel, R.K., Patan, R., Gandomi, A.H., Sankayya, M. and Balusamy, B., 2020. Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. *Neural Computing and Applications*, *32*, pp.639-647.

[26] Abunadi, I. and Kumar, R.L., 2021. BSF-EHR: blockchain security framework for electronic health records of patients. Sensors, 21(8), p.2865.

[27] Alonso, S.G., Arambarri, J., López-Coronado, M. and de la Torre Díez, I., 2019. Proposing new blockchain challenges in ehealth. Journal of medical systems, 43, pp.1-7.

[28] Majeed, U., Khan, L.U., Yaqoob, I., Kazmi, S.A., Salah, K. and Hong, C.S., 2021. Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges. Journal of Network and Computer Applications, 181, p.103007.