International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An IoT and Blockchain-Based Secure Medical Care Framework Using Deep Learning and Nature-Inspired Algorithms

Harjinder Singh[1], Zahid Ahmed[2], Mayank Deep Khare[3], Bhuvana J.[4]

Submitted:19/04/2023 **Revised:**12/06/2023 **Accepted:**21/06/2023

Abstract*:* A secure medical care infrastructure built on the Internet of Things (IoT) and Blockchain can improve the security, privacy, and interoperability of healthcare systems and patient data. A similar structure can take advantage of the positive aspects of both Blockchain (BC) and IoT technology to meet the particular needs and challenges of the healthcare sector. In this study, we suggested the IoT-based blockchain-based safe medical care system employing deep learning and nature-inspired algorithms. In the first stage of the study, a blockchain-based secure data storage system, user authentication, and health status prediction are presented. Dwarf mongoose optimization (DMO) is used for feature extraction and feature selection after min-max normalization has been applied to the data. The health status is classified into normal and abnormal states using the improved bumble bee mating optimization algorithm with bi-long short-term memory (IBBMO-Bi-LSTM). Temporarily, the out-of-the-ordinary measurements are kept in the relevant patient blockchain. Here, medical data is safely stored for further study using blockchain technology. The suggested model is validated by contrasting it with different baseline methodologies and has an accuracy rate, encryption, and decryption time. The proposed methods achieve a security level in terms of security.

Keywords: *IoT, Blockchain, health status prediction, Dwarf mongoose optimization (DMO), improved bumble bee mating optimization algorithm with bi-long short-term memory (IBBMO-Bi-LSTM)*

1. Introduction

Blockchain, wearable tech, and the Internet of Things are just a few examples of the cutting-edge technologies that have contributed to the healthcare industry's recent explosion of growth. Many aspects of healthcare, such as electronic medical records, remote patient monitoring, disease prediction, patient tracking, medicine tracing, and the fight against infectious diseases like the COVID-19 pandemic, have profited from this technology. As more IoT devices are used, more data is handled across the network, which presents security and privacy threats. Several studies have recommended implementing Blockchain to protect IoT networks. BC decentralized and distributed nature and the cryptography utilized during its development have piqued the curiosity of those looking to keep private information safe and secure [1]. The distributed ledger technology known as BC offers a safe means to conduct and record business transactions and contracts. It offers a highly secure, immutable, and encrypted record-keeping system while being consensus-driven and trustless. It evolved from the public, distrustless, anonymous, but extremely secure Bitcoin crypto-currency network. Business BC, or private BC, has been introduced and may be used in industrial processes. A promising approach, BBC can greatly enhance and optimize several features of intelligent procedures when information or data is transferred [2]. B.C. technology is a distributed ledger system that can establish trustworthy and agreeable peer-to-peer (P2P) networks. On the one hand, the Blockchain uses a decentralized consensus technique to obtain an agreement for transactions amongst individual users, thus mitigating the issues of a trustless distributed environment. However, traditional encryption methods negatively impact the user experience because they prevent users from performing searches. Searchable encryption algorithms have been developed in symmetric-key and public-key settings to safeguard data searches over encrypted medical data. There are still some unresolved issues with patient or medical professional keyword searches over the encrypted medical data, even though the symmetric-key option is more effective than the public-key configuration. The key issues that threaten medical data security are the lack of a responsible third party for effective storage, retrieval, and querying of the data, problems with user-side verification (the patient should be

1Assistant Professor, College of Computing Science and Information Technology, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India, Email id: harjinder.mca07@gmail.com

2Assistant Professor, Department of Computer Science & Application, Vivekananda Global University, Jaipur, India, Email Id: zahid.a.me@vgu.ac.in

3Assistant Professor & HoD, Department of Internet of Things (IoT), Noida Institute of Engineering and Technology, Greater Noida, Uttar Pradesh, India, Email id: mayank@niet.co.in

4Associate Professor, Department of Computer Science and IT, Jain(Deemed-to-be University), Bangalore-27, India, Email Id: j.bhuvana@jainuniversity.ac.in

a legitimate user), and problems with server-side verification. However, the decentralized blockchain system may guarantee security by employing digital signatures and encryption-based hashing algorithms [3]. Due to its commercial nature, it is essential to ensure medical data's integrity, security, and privacy. As a result, an effective and secure framework for data management was needed. Due to adverse risks associated with disclosing the specifics of their data, the CSP disputed the need for collaboration in exchanging medical data. The real threat to data managers and owners is when attacker data users' controls leak received data. Numerous cryptographic algorithms have been created to safely exchange and store healthcare data to deal with these difficulties, but they have fallen short. The cryptographic techniques consider both the user's data's privacy and the unreliability of the cloud server. Before outsourcing data to a cloud server, encryption must be performed. Conversely, traditional encryption methods negatively impact the user experience because they prevent users from performing searches. Using symmetric-key and public-key infrastructures, searchable encryption algorithms have been developed to safeguard data searches over encrypted medical data. While keyword searches over encrypted medical data are generally more secure with the symmetric-key option than with the public-key configuration, some issues remain to be resolved. Several issues put medical data at risk, including the need for user-side verification, server-side verification, and the absence of a responsible third party for efficient data storage, retrieval, and querying [4]. Healthcare providers produce enormous amounts of data in several formats, including records, economic papers, the results of clinical tests, images from imaging tests, assessments of vital signs, etc. The vast database built in healthcare environments is increasing, even though several issues plague data access to healthcare information, and there are other ways to collect information. Blockchain offers the capability to improve the authenticity and verification of the data. Additionally, it aids in data dissemination throughout the network or services. These applications impact the price, data quality, and significance of healthcare delivery within the system. A decentralized, transparent network without a middleman is Blockchain. Blockchain-based healthcare networks don't require several levels of authentication because everyone using the blockchain infrastructure can access the data. Data is made public and accessible to users. Such advancements will resolve the healthcare industry's many issues [5]. We proposed a decentralized, BC-based and physics-inspired system for providing medical care over the IoT Things. Using an enhanced bumble bee mating optimization algorithm with bi-long short-term memory (IBBMO-Bi-LSTM), the health status is divided into normal and abnormal categories.

2. Related Work

According to the research [6], a machine learning technique known as Sine Cosine Weighted K-Nearest Neighbor (SCA_WKNN), which learns from data stored in blockchains, is offered to predict heart illness. The research [7] concentrated on information on the diagnosis and prognosis of diabetic retinopathy. The chronic condition known as diabetic retinopathy, which is brought on by diabetes, results in total blindness. The state must be diagnosed early to lessen the likelihood of visual loss. This study offers a unique two-part model to ease any security and privacy worries in the Internet of Healthcare Things [8]. The first section uses machine learning to analyze a patient's health indicators, find and discard anomalous data, and record the non-anomalous data together with discoveries in a transparent, secure manner utilizing Blockchain. The research [9] suggested a safe and anonymous biomedical image processing system built on a blockchain. This study [10] provided an original structure for efficiently using shareable resources within the reachable region to construct an opportunistic computing system while protecting user privacy. The research [11] suggested tool's target is identifying attacks on the healthcare cyber-physical system. The placement and initial generation of the sensor nodes in this method is done using the wise greedy routing strategy. The research [12] suggested framework applies the idea of fog computing to applications that require fast response times. In addition, a hybrid classifier is employed to identify swine flu cases early on and provide alerts to the patients' guardians and public health agencies. With an emphasis on big data technologies, this study [13] attempts to explain new advancements. It approaches suitable in various fields while revealing the trust management strategies now used in IoT. A study [14] suggests that natural optimization algorithms could be crucial in addressing the multiple aspects of healthcare. In the event of future pandemics, the insights from our chapter may enable healthcare decision-makers, physicians, and other interested parties to prioritize better and develop efforts to operationalize A.I. The research [15] aimed to provide a safe critical generation procedure for data-sharing by utilizing the Rider Horse Herd Optimization Algorithm (RHHO). Study [16] combined cutting-edge breakthroughs in agricultural and human healthcare, including improvements in intelligent algorithms and productive IoT applications. The research [17] presented an improved chaotic salp swarm optimization method (ECSSA) and LightGBM classifier as an effective intrusion detection mechanism for the message queuing telemetry transport-IoT networks.

The remaining sections of this research are as follows: Part 2 contains the related works; the proposed methodology is introduced in Part 3; the result and discussion of the study are in Part 4; the conclusion is in Part 5.

3. Proposed Methodology

Consider a typical IoT scenario in the healthcare industry where several IoT devices, including a thermostat and intrusion detection system, are connected to a database server. The suggested paradigm comprises many states that include end IoT devices and is linked to the medical data center via blockchain technology. In this study, usage cases for data access and administration are taken into account. IoT devices should be able to access one another based on access rights, or Alice should be able to view temperature data remotely. Figure 1 depicts the systematic representation of the suggested method.

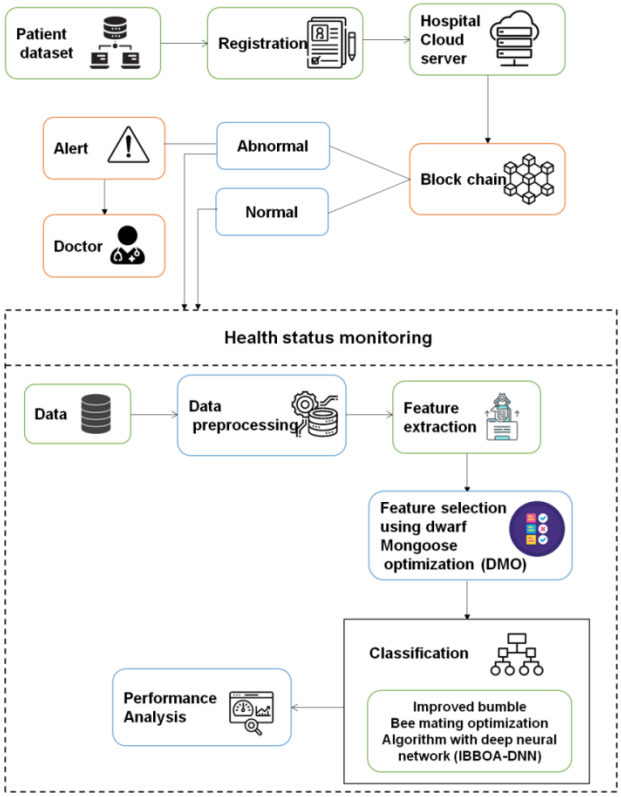

Fig.1. Systematic representation of the suggested method

3.1. Registration Phase

In the first stage, the patient's information is entered into the cloud server at the hospital. A patient's unique I.D. is created after a successful registration. The patient is then sent their login and password, the hashed combination of their unique I.D., timestamp (the time the patient registered), and other data using the Adler-32 hashing technique. The hash code will be used for patient authentication during login. Adler-32 is a hashing algorithm where two approximated checksums, G and H, each consisting of 16 bits, are combined to produce a 32-bit result. When counting bytes, H equals the sum of the distinct G values at each stage. Initial values for G and H are 1 and 0, respectively. Future examples will show how hash codes are generated.

Let β be the patient's unique I.D., and let S represent the patient's timestamp at registration time. Let α define the byte phrase for which the authentication must be calculated. Hash codes are generated by combining the patient's I.D. and timestamp. It is depicted below.

$$\alpha = \beta S \quad (1)$$

The Adler-32 hashing method, theoretically defined below, is then used to create the hash code for the concatenated values. In this case, 65521 is the most significant prime number below 2^{16}.

$$H = 1 + \alpha_1 + \alpha_2 \ldots\ldots\ldots + \alpha_m . |65521| \quad (2)$$

Here, G is the total of each value of H, where n stands for the length of α.

$$G = \langle (1 + \alpha_1) + (1 + \alpha_1 + \alpha_2) + \cdots + (1 + \alpha_2 + \cdots + \alpha_m) \rangle . |65521| \quad (3)$$

The following is how the hash code is created:

$$Adl(\alpha) = (G \times 65521) + H \quad (4)$$

$Adl(\alpha)$ displays the Adler-32 hash-coded value in (4). The patient will also receive this hash code used for data encryption, decryption, and user authentication during login. Once registration is complete, the Blockchain provides people's information privacy and security by storing the patient's registration data.

3.2. Blockchain

The rapid expansion of the medical business has made it difficult to manage patient privacy while storing, distributing, and managing medical information. The BC offered a potential remedy for these problems, which involved securely exchanging medical data. A decentralized data structure is called BC. By creating a digital ledger, it makes transactions permanent and irrevocable. The catalog contains a sequence of blocks that are cryptographically connected. After being recorded in the B.C. ledger, data blocks cannot be modified or removed. A linked list of encrypted transactions (using a hash instead of a reference) safeguards the vast bulk of B.C.'s data. B.C. technique employs a hash function that generates a hash value by encrypting the input data with the Secure Hash Algorithm 256. It will be apparent if an attacker has tampered with a block and what they changed it to. The blockchain proof-of-work (POW) system contributes to the growth of a trustworthy consensus system. Editing or changing a blockchain would be computationally expensive, making it difficult for a hostile attacker to do so. To add a new block to the B.C. network, a proof-of-work (POW) must be solved.

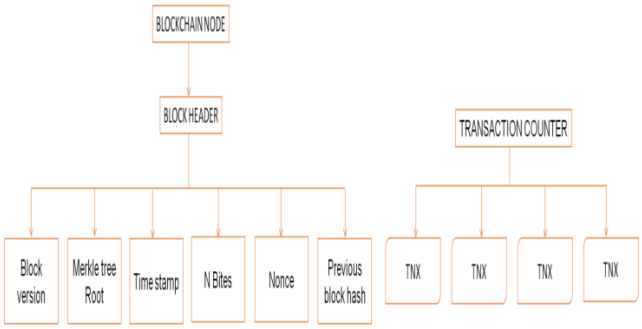

Fig.2. Basic structure of BC

Fig. 2 illustrates the B.C. structure. Bytes in the first portion imply that the block size is shown. A block header is then used to record the information, including the Merkle root, the B.C. version, and the H.C. of the previous block. The Merkle source refers to the hash value located at the heart of the Merkle tree. All the transactions in the final part of the block are organized into a tree-like structure known as a Merkle tree. The block header also contains the current date, the difficulty target (POW), and the nonce (any random value for POW).

3.3. User Authentication

The information entered during registration and login is compared during this stage. The user will be verified if both match and the data is felt. If the two don't match, an error warning will appear, and the data won't be detected until authentication occurs. After a successful patient verification, the wire-free body sensors (WBS) gather patient health data. The quality of human life has improved. However, IoT devices do not ensure user privacy while transferring data via wireless transmission. Data encryption is therefore required during data exchange.

3.4. Encryption

The data are secured using,

$$\Omega = N.\log(\delta) * mod(Q) \quad (5)$$

N denotes the initial human sensing input in Equation (5), and Ω indicates the encrypted data.

3.5. Decryption

The encrypted data is decoded in the document system, centered on the Equation below,

$$N = \Omega.\log(\delta) * mod(Q) \quad (6)$$

As a result, the physician's system receives the encrypted patient

data from the cloud server, which is decrypted. Then, H.S. prediction is performed using this data.

3.6. Medical Condition Assessment

Participant identification number: Participants can categorize each unit using a standard blockchain framework (health workers and patient facts are connected through the blockchain structure). Data inputted into the machine is permanent and defines the information provided by each computer separately. These IoT devices should also be able to store data in cloud storage based on access controls. Before discussing the model details in Table 1, let's include all the stages.

Table 1. Descriptive of the dataset

S.NO.	Data sets	Alerts	IoT technology	Parameters use
1	Sensor-based health datasets	High blood pressure	Blood pressure sensor	Blood pressure
2		High temperature	Temperature sensor	Temperature
3		ECG problem	ECG sensor	ECG
4		EMG problem	EMG sensor	EMG
5		High pressure	Pressure sensor	Pressure
6		Visual problem	Visual sensor	Visual
7		High respiration	Respirations sensors	Respiration
8		High heart rates	Heart rate sensor	Heart rates

3.7. Data preprocessing

Users must give data preparation since the device data set contains some incorrect or duplicate information and form during individual potential, which includes normalization and managing any inaccurate data, errors, and similar data. Using an equation to standardize the medical data information OP^{mg} inside the domain [0, 1] helped cut down on computing costs:

$$Data\_O_{norm} = \frac{OP^{mg} - Data\_O_{min}}{Data\_O_{max} - Data\_O_{min}} \times [max_{value} - min_{value}] + min_{value} \quad (7)$$

Where $Data_{O_{norm}}$ represents the normalized value of a data source, Information $Data\_O_{min}$ represents the minimum value of a dataset, $Data_{O_{max}}$represents the maximum value of a dataset, OP^{mg} represents the original value of the medical data source, max-value, and min-value represents the range of a normalized input data, with max-value = 1 and min-value = 0, and O.P. means the initial cost of an anomaly data source.

3.8. Feature extraction

After the data has been preprocessed, the features are extracted to facilitate the classification process and enhance its efficacy. The total number of elements in the dataset is decreased by the F.E. Only the most helpful information from the entire set is summarized in this section. In terms of the retrieved features (t_j),

$$t_j = t_1, t_2, \dots\dots, t_m \tag{8}$$

The number of features recovered from the input dataset is denoted by m in (8).

3.9. Feature selection using Dwarf Mongoose Optimization Algorithm

The dwarf mongoose, or Helogale, inspires the foraging and social behavior of the population-based randomized metaheuristic approach DMO. DMOs don't work together when searching for food like they do when foraging. Because these animals are semi-nomadic, it makes sense for them to construct sleeping mounds close to a plentiful food source. To address optimization issues, the program simulates this animal's way of existence statistically.

Random initialization is used at the beginning of every population-based optimization technique. After then, every solution congregates around the world's best optima due to the intensification and diversification criteria. Like the DMO, the mongoose's candidate population is initialized when the DMO begins its solution. This population is produced stochastically between a specific task's lower and upper boundaries.

$$V = \begin{bmatrix} v_{1,1} & v_{1,2} & \cdots & v_{1,c-1} & b_{1,c} \\ v_{2,1} & v_{2,2} & \cdots & v_{2,c-1} & v_{2,c} \\ \vdots & \vdots_{v_{ji}} & \vdots & \vdots & \\ v_{m,1} & v_{m,1} & \dots & v_{m,c-1} & v_{m,c} \end{bmatrix} \tag{9}$$

Where m is for the population size, $v_{m,c}$ stands for the location of the m^{th} dimension of the $c$ity population, and c stands for the extent of the problem. In (10), v represents a randomly created pool of potential candidates for the open position.

$$v_{m,c} = unifrnd(VarMin, VarMax, VarSize) \tag{10}$$

$VarMin$ and $VarMax$ are the minimum and maximum allowed values, and $VarSiz$e is the dimensions of the issue. Uniformly distributed random numbers are represented by $unified$. Each iteration improves upon the previous best answer identified.

The DMO follows the standard two-stage structure of other metaheuristic algorithms, consisting of "exploration" and "exploitation," or "intensification" and "exploration," respectively. The DMO's three core social structures—the alpha group, the scout group, and the babysitters—carry out activities at both levels. Using criterion (11), the alpha female is chosen.

$$\alpha = \frac{ejs_j}{\sum_{j=1}^{m} ejs_j} \tag{11}$$

There are precisely $m - ej$ mongooses in the elite alpha tier. The female alpha makes a sound called a peep to lead the rest of the pack, where ej represents the number of babysitters. In (12), the sleeping mound is determined by a phrase signifying plentiful food.

$$V_{j+1} = V_j + phi * peep \tag{12}$$

The sleeping mound is evaluated after each iteration in the case where $a\,phi$ is a random number with uniform distribution [1,1], (13) illustrates this:

$$tn_j = \frac{ejs_{j+1} - ejs_j}{max\{|ejs_{j+1}, ejs_j|\}} \tag{13}$$

Equation (14) is used to get an average value once a dormant mound is woken up.

$$\varphi = \frac{\sum_{j=1}^{m} tn_j}{m} \tag{14}$$

Once the criteria for changing the babysitter are met, the second phase involves scouting, wherein the prospective food value of the next sleeping mound is assessed. Because mongoose is notorious for not returning to their previous sleeping mounds, the scouting party is constantly on the lookout for the next one. With the rationale that the further the unit forages, the more likely it is to find the following sleeping mound, it is well-documented that mongooses in DMO forage and scout simultaneously. This is modeled in (15).

$$V_{j+1} = \begin{cases} V_j - DE * phi * rand * \left[V_j - \vec{N}\right] if\ \varphi_{j+1} > \varphi_j \\ V_j - DE * phi * rand * \left[V_j - \vec{N}\right] \quad else \end{cases} \tag{15}$$

Here, a random number between 0 and 1 and a decreasing parameter, denoted by D.E., governs the collectively volatile movements of a group of mongooses$DE = \left(1 - \frac{iter}{Max\ iter}\right)^{\left(2\frac{iter}{Max\ iter}\right)}$. The force that prompts a mongoose to move to a new sleeping mound can be $\vec{N} = \sum_{j=1}^{m} \frac{V_j \times tn_j}{V_j}$, where m is the number of mongooses. While the other group tends to the young animals, the scouts and foragers search for a resting mound and food. The number of applicants is reduced by one because they wait until the babysitting exchange parameter in (16) is reached before beginning their foraging or scouting efforts.

3.10. Classification using IBBMOA-Bi-LSTM

The suggested approach, Bumble Bees Mating Optimization (BBMO), is built upon the Bi-LSTM. Proper mapping of the chosen problem is used to provide the answer, referred to as a bee (queen, worker, or drone). The

steps of a BBMO algorithm are as follows:

- **Initialization:** Randomly selecting the starting bumble bee population and evaluating fitness function.
- **Drones' Selection:** The queen chooses the drones that will be used for mating.
- **Offspring' Creation:** The new queens, workers, and drones of three different species of bumble bees are produced utilizing multiparent crossover, mutation operator, and workers.
- **Meet the new monarchs:** Broods are fed to increase their fitness so that the strongest survivors can mature into new queens. The rest of the group will soon get to work. This is done by using combinatorial neighborhood topology (CNT) for the first analytical exposition of combinatorial neighborhood topology and using combinatorial neighborhood topology within the context of a BBMO algorithm.

If the new queen eats from a worker or the old queen can be predicted with the help of the following equations:

$$K_1 = (w_{bound} - k_{boumd}) \times \left(u_1 - \frac{u_1}{iter_{max}} \times s\right) + k_{bound} \quad (16)$$

$$K_2 = (w_{bound} - k_{boumd}) \times \left(u_2 - \frac{u_1}{2*iter_{max}} \times s\right) + k_{bound} \quad (17)$$

Where the upper and lower bounds are w_{bound}, and k_{bound} and s r symbolize the current iteration. Itermax indicates the maximum amount of iterations. The range of the variables K_1 and K_2 are determined by the parameters u_1 and u_2. The value of u_2 should be greater than the value of u_1, and the importance of K_2 should be more than $that\ of\ K_1$. The following Equation yields the feeding selection:

$$smp_j(s) = \begin{cases} p_j(s), & if\ rand_j, (k,a) \le K_1 \\ uq_j(s), & if K_1 \le rand_j \le K_2 \\ mp_j(s)\ or\ up_i, & otherwise. \end{cases} \quad (18)$$

Where p is the current queen and is a potential new queen, mp_j is a contender for the new queen in the brood, and uq_j and uq_i are two separate workers.

- **Mutation phase:** The new queens depart the hive after this. After that, the Variable Neighborhood Search (VNS) algorithm executes a mutation phase.
- **Mating phase:** The quantity of drones in each external generation per colony is:

$$`number\ of\ drones\ per\ colony = \frac{number\ of\ drone}{number\ of\ queens} \quad (19)$$

The drones then depart from the hive, searching for fresh queens to mate with. Bi-LSTM uses the Iterated Local Search (ILS) algorithm when the drones travel away from the pack.

- **Next Iteration:** Only the most fertile queens will pass on their genes to the next generation.

The suggested technique made use of Bi-LSTM algorithms. An RNN version called the LSTM is primarily used to address the context dependency issue. The two LSTMs that makeup Bi-LSTM are front and backward. A single LSTM can only get past information instead, of a one-direction LSTM, which cannot acquire future knowledge. As a result, reversible LSTM may recover more specific characteristics than southbound LSTM. A pair LSTMs makes up a Bi-LSTM. As a result, LSTM is the present state g_{is} derived from either the remembrance light's value $e_{(s)}$, the recollection door's value $j_{(s)}$, the cell state $d_{(s)}$, the temporary cell state $h_{(s)}$, and the instruction set $p_{(s)}$. Finally, Bi-LSTM takes the g_s of the two LSTMs moving in different directions and combines them to get the outcome at time t. The following is the calculating formula:

$$e_{(s)} = \delta(Z_e y_{(s)} + v_e g_{(s-1)} + a_e \quad (20)$$

$$j_{(s)} = \delta(Z_e y_{(s)} + v_j g_{(s-1)} + a_e) \quad (21)$$

$$h_{(s)} = \tan g\ (Z_h y_{(s)} + v_h g_{(s-1)} + a_h) \quad (22)$$

$$d_{(s)} = e_{(s)} \times d_{s-1} + j_{(s)} \times h_{(s)} \quad (23)$$

$$p_{(s)} = \delta(Z_p y_{(s)} + v_j g_{(s-1)} + a_p) \quad (24)$$

$$g_s = p_{(s)} \times tang\ (d_s) \quad (25)$$

Where Z represents the weight, and a represents the offset.

One of the most excellent methods is the Bi-LSTM. Bi-LSTM models, as compared to bidirectional LSTM models, are often more efficient in dealing with the relevant information because their output at any one time is reliant on the preceding and incoming segments. The Bi-LSTM concept uses LSTM units in a forward and a backward layer to understand prior and future information. The Bi-LSTM structure is shown in Figure 3.

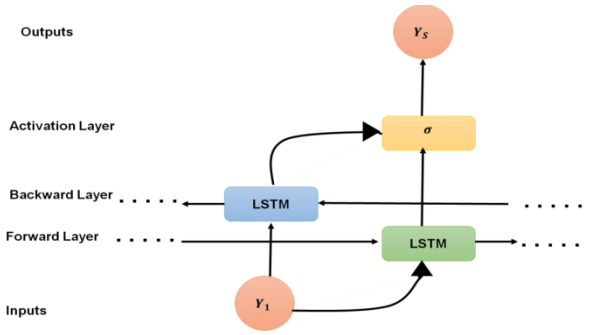

Fig.3. Bi-LSTM structure

Seven different outputs were generated using a combination of linked variables, LSTM and Bi-LSTM, with two hidden layers. To build the models, we used the following parameters: (a) 5000 iterations; (b) a dropout rate of 0.2; (c) an Adam optimizer with a begin learning approach of 0.01; and (d) a mini-batch size of 128. The category pass error rate described in Equation was also used (25),

$$K(x', x) = \sum_{j=0}^{L} xj.\log(x'j) \quad (26)$$

$$I(\Omega) = \frac{1}{n}\sum_{j=1}^{n} K(x', x) \quad (27)$$

Where j is the constituent amount, x is the actual label, L is the total number of classes, and x' is the predicted label. Equation (27) also shows the cost of generalizing the gradient descent behavior, where n represents the total number of parts and the Ω entire set of values. The SOM-Bi-LSTM was used to evaluate the classification reliability, with the lowest being the best performance.

4. Result And Discussion

In this study, the proposed method is implemented in Python, and its efficacy is compared to that of previously used approaches such as convolutional neural networks (CNN), deep neural networks (DNNs), and orthogonal particle swarm optimization with deep neural networks (OPOS-DNNs). Accuracy, security level, encryption, and decryption time were important metrics studied using proposed and current approaches.

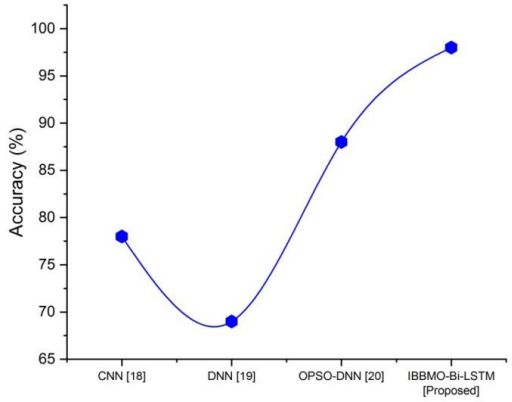

Fig.4. Comparison of accuracy

Fig. 4 displays the accuracy of the proposed and existing methods. It measures how well the model did overall in terms of all the tested samples. When testing a hypothesis, we divide the number of correct responses by the total number of possible answers.

$$Accuracy = \frac{TP+TN}{TP+FP+FN+TN} \quad (28)$$

The proposed IBBMO-Bi-LSTM approach was more accurate than the existing methods, including CNN, DNN, and OPOS-DNN.

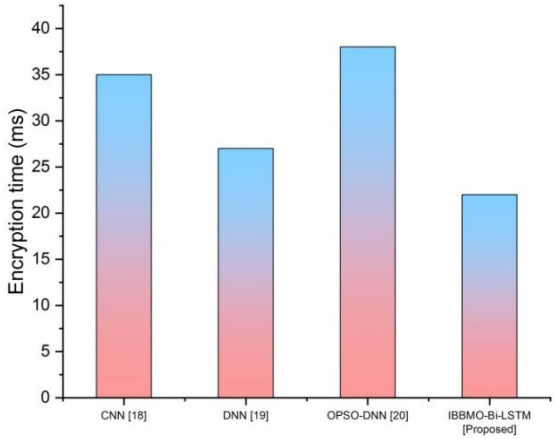

Fig.5. Comparison of encryption time

The disparity in encryption times is shown in Figure 5. How long it takes to encrypt data depends on several factors, including the amount of data being encrypted, the availability of computational resources, the desired level of security, and the encryption method. In general, more secure encryption methods take more time to encrypt data. The proposed IBBMO-Bi-LSTM encrypts data faster than current methods like CNN, DNN, and OPSO-DNN.

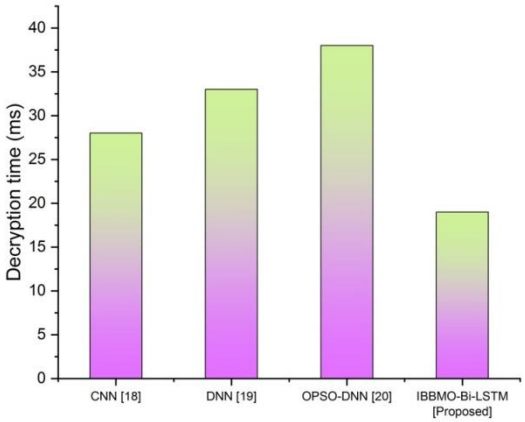

Fig.6. Comparison of decryption time(ms)

Fig. 6 compares decryption times. The decryption algorithm, data amount, processing resources, and security level affect decryption time. Like encryption, decryption can take milliseconds for small data sets using fast

algorithms, seconds or minutes for larger data sets, or computationally intensive techniques. Current encryption methods and enough processing power should make decryption fast in most real-world settings. Thus, IBBMO-Bi-LSTM has the fastest decryption time of CNN, DNN, and OPSO-DNN.

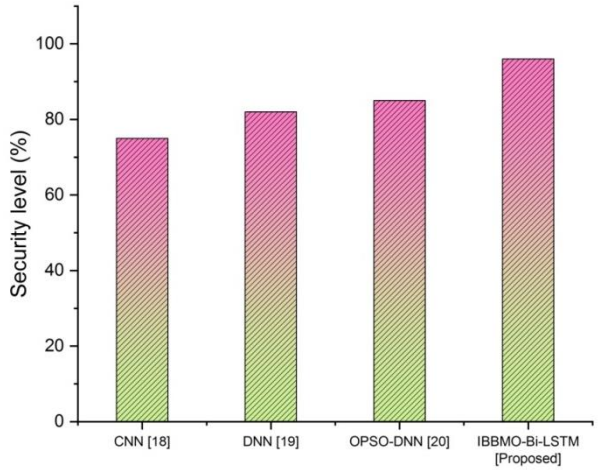

Fig.7. Comparison of security level

Fig. 7 depicts the comparison of security levels. Security requires data integrity and authentication. High, medium, and low security exists. Key size and algorithm determine encryption security. It resists brute force, cryptanalysis, and computational cryptographic attacks. Complexity and key size assess safety. Strong encryption defies computation and mathematical errors. Security makes decrypting data without the key difficult. The suggested work IBBMO-Bi-LSTM has the highest security level of CNN, DNN, and OPSO-DNN.

5. Conclusion

This system includes user identification, an health status prediction engine, and a secure data storage system centered on Blockchain technology. Health status monitoring, data encryption, and Blockchain are only some of the components of the proposed method. Patient's medical records are kept confidential using blockchain technology. A health status monitoring system is made for predicting the patient's health status. For safely transporting patient IoT data in the computer system, IBBMO-Bi-LSTM is suggested as the data encryption method. This experiment examined various measurements, including accuracy, security level, encryption, and decryption. Performances were measured by comparing the results with some baseline procedures. IBBMO-Bi-LSTM was suggested, and the findings were 98% accuracy, 96% security level, 45 ms of encryption time, and 38% decryption time. Comparing the proposed method to the highest standards reveals superior performance, security, accuracy, and time saved. In the future, we plan to employ state-of-the-art deep learning methods to optimize the job regarding data volume and network outages. The suggested framework will also be used in other IoT application scenarios.

References

[1] Azbeg K, Ouchetto O, Andaloussi SJ, Fetjah L. A taxonomic review of the use of IoT and blockchain in healthcare applications. Irbm. 2022,43(5):511-9.

[2] Biswas S, Sharif K, Li F, Maharjan S, Mohanty SP, Wang Y. PoBT: A lightweight consensus algorithm for scalable IoT business blockchain. IEEE Internet of Things Journal. 2019;7(3):2343-55.

[3] Cao B, Li Y, Zhang L, Zhang L, Mumtaz S, Zhou Z, Peng M. When Internet of Things meets blockchain: Challenges in distributed consensus. IEEE Network. 2019, 33(6):133-9.

[4] Mahajan HB, Rashid AS, Junnarkar AA, Uke N, Deshpande SD, Futane PR, Alkhayyat A, Alhayani B. Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems. Applied Nanoscience. 2023, 13(3):2329-42.

[5] Agbo Shynu PG, Menon VG, Kumar RL, Kadry S, Nam Y. Blockchain-based secure healthcare application for diabetic-cardio disease prediction in fog computing. IEEE Access. 2021, 9:45706-20.

[6] Hasanova H, Tufail M, Baek UJ, Park JT, Kim MS. A novel blockchain-enabled heart disease prediction mechanism using machine learning. Computers and Electrical Engineering. 2022, 101:108086.

[7] Uppamma P, Bhattacharya S. Diabetic Retinopathy Detection: A Blockchain and African Vulture Optimization Algorithm-Based Deep Learning Framework. Electronics. 2023, 12(3):742.

[8] Das, S., Karmakar, S. and Saha, H.N., Secure Digital Health Data Management in Internet of Things Using Blockchain and Machine Learning. In Digital Health Transformation with Blockchain and Artificial Intelligence. 2022, pp. 23-45. CRC Press.

[9] Mahajan HB, Junnarkar AA. Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing. Multimedia Tools and Applications. 2023, 15:1-24.

[10] Dhasarathan C, Kumar M, Srivastava AK, Al-Turjman F, Shankar A, Kumar M. A bio-inspired privacy-preserving framework for healthcare systems. The Journal of Supercomputing. 2021, 77:11099-134.

[11] Kumar CV. A real time health care cyber attack detection using ensemble classifier. Computers and

Electrical Engineering. 2022, 101:108043.

[12] Singh PD, Kaur R, Singh KD, Dhiman G, Soni M. Fog-centric IoT based smart healthcare support service for monitoring and controlling an epidemic of Swine Flu virus. Informatics in Medicine Unlocked. 2021 Jan 1;26:100636.

[13] Fabi AK, Thampi SM. Secure Big Data Transmission with Trust Management for the Internet of Things (IoT). Combating Security Challenges in the Age of Big Data: Powered by State-of-the-Art Artificial Intelligence Techniques. 2020:1-27.

[14] Siddiqui MF, Alam A, Kalmatov R, Mouna A, Villela R, Mitalipova A, Mrad YN, Rahat SA, Magarde BK, Muhammad W, Sherbaevna SR. Leveraging Healthcare System with Nature-Inspired Computing Techniques: An Overview and Future Perspective. Nature-Inspired Intelligent Computing Techniques in Bioinformatics. 2022, 1:19-42.

[15] Yempally S, Singh SK, Sarveshwaran V. A secure and efficient authentication and multimedia data sharing approach in IoT-healthcare. The Imaging Science Journal. 2023, 4:1-22.

[16] Bharti V, Biswas B, Shukla KK. Computational intelligence in Internet of things for future healthcare applications. InIoT-Based Data Analytics for the Healthcare Industry 2021. pp. 57-78. Academic Press.

[17] Prajisha C, Vasudevan AR. An efficient intrusion detection system for MQTT-IoT using enhanced chaotic salp swarm algorithm and LightGBM. International Journal of Information Security. 2022, 21(6):1263-82.

[18] M., Li, Z., & Ali, H. A., Facefilter: face 1. Qi, P., Chiaro, D., Giampaolo, F. and Piccialli, F., 2023. A blockchain-based secure Internet of medical things framework for stress detection. Information Sciences, 628, pp.377-390.

[19] Somayaji, S.R.K., Alazab, M., Manoj, M.K., Bucchiarone, A., Chowdhary, C.L. and Gadekallu, T.R., 2020, December. A framework for prediction and storage of battery life in IoT devices using DNN and blockchain. In 2020 IEEE Globecom Workshops (GC Wkshps (pp. 1-6). IEEE.

[20] Veeramakali, T., Siva, R., Sivakumar, B., Senthil Mahesh, P.C. and Krishnaraj, N., 2021. An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model. The Journal of Supercomputing, pp.1-21..

[21] Ibrahim, S. S. ., & Ravi, G. . (2023). Deep learning based Brain Tumour Classification based on Recursive Sigmoid Neural Network based on Multi-Scale Neural Segmentation. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2s), 77–86. https://doi.org/10.17762/ijritcc.v11i2s.6031

[22] ARECHE, F. O. ., & Palsetty , K. . (2021). Ubiquitous Counter Propagation Network in Analysis of Diabetic Data Using Extended Self-Organizing Map. Research Journal of Computer Systems and Engineering, 2(2), 51:57. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/33