JOIN (Jurnal Online Informatika)
p-ISSN: 2528-1682, e-ISSN: 2527-9165
Volume 10 Number 2 | December 2025: 418-431
DOI: 10.15575/join.v10i2.1638

Blockchain-Enabled Secure Healthcare Data Management with Modified Gazelle Optimization and DLT-Trained RNN-BILSTM Approach

Rolly Saxena[1], D. Srinivasa Rao[2]
[1]Department of Computer Applications, Medi-Caps University, Indore, Madhya Pradesh, India
[2]Department of Computer Science and Engineering, Medi-Caps University, Indore, Madhya Pradesh, India

Article Info

Article history:

Received May 12, 2025
Revised June 15, 2025
Accepted July 13, 2025
Published November 10, 2025

Keywords:

Blockchain
Healthcare data
Modified Gazelle Optimization
Distributed Ledger Technology
RNN-BILSTM based IDS

ABSTRACT

The growth of the healthcare system has posed challenges in safeguarding patient privacy amidst the storage, distribution and management of medical data. Blockchain (BC) offers a promising result by securely enabling the exchange of medical information. Utilizing block chain technology ensures the security of individuals' confidential health information. The use of a decentralized, immutable ledger using blockchain technology provides a secure, impenetrable platform for storing and retrieving private medical information, protecting patient privacy. The application of Modified Gazelle Optimization enables the determination of the shortest path for efficient data transfers within the block chain network. By adopting a specialized routing protocol called Modified Gazelle Optimized Routing, this approach minimizes latency and maximizes throughput, facilitating continuous and expedited transfer of health data across the network. To assure the data confidentiality and integrity of network nodes, a Distributed Ledger Technology (DLT) trained Recurrent Neural Network with Bidirectional Long Short Term Memory (RNN-BILSTM) approach is implemented. This advanced Deep Learning (DL) technique enhances the security and reliability of the network by detecting and preventing unauthorized access and tampering attempts. The proposed RNN-BILSTM based Intrusion Detection System (IDS) efficiently detects different types of attacks with high accuracy. By analyzing network traffic and patterns in real-time, the IDS have the ability to identify and mitigate harmful Internet of Things (IoT) requests and various stealthy attack types, including previously unknown threats. The outcomes of this research prove an efficacy and consistency of the proposed strategy in enhancing the security, efficiency and performance matrix with an accuracy of 97% and comparative analysis is done with traditional methods, thereby ensuring an availability and integrity of healthcare data.

Corresponding Author:

Rolly Saxena,
Computer Applications Department, Research Scholar, Medi- Caps University, Indore, Madhya Pradesh, India.
Email: rollysaxena2@gmail.com

1. INTRODUCTION

The healthcare system is composed of multiple organizations that maintain patient health information in a system that is protected by a number of regulations. Safeguarding health data is becoming progressively challenging due to the involvement of several hackers and the harm that natural

disasters are causing to system nodes. Effective data exchange, safeguarding safe data storage, and smooth provider collaboration are frequently challenges for traditional healthcare systems [1-2]. The IoT, Blockchain, and Edge Computing are a few examples of emerging technologies that have played a significant role in the development of smart health systems [3]. In light of the growing need for digital data protection across all domains in recent years, blockchain technology has emerged as one of these that is more adaptable than other technologies [4–7]. Therefore, in integrated domain contexts, healthcare providers will benefit from an extremely protected health data ledger provided by a cyber-safeguard scheme based on blockchain technology [8–11]. For efficient transfer of data in a block blockchain network to find the shortest path, various routing protocols are used. For reliable IoT data transit in healthcare systems, [12] presents a priority-based energy-efficient routing protocol. The most important information is the emergency situation, which needs to be effectively transferred as soon as possible. Vital health data is intended to be P2 priority data, meaning that it requires less real-time processing than emergency data. On the other hand, it should appropriately raise the weight values of the residual energy parameters and decrease energy consumption as the premise for P2 priority data. By introducing a configuration of relay and sensor nodes attached to the human body based on the postural movement of patients, an enhanced QoS-aware routing protocol for WBAN is developed in [13]. This allows the protocol to select the most practical path and significantly increases the network lifetime. Because it concentrates on enhancing signal quality, packet delivery, and energy efficiency, it adds more complexity. In order to minimize transfers among the medical server and the sensor nodes, [14] introduced an EERP-DPM for healthcare utilizing the IoT. As long as the forecasts agree with the readings, this method enables the sensor nodes to forego sending their detected data to the Medical Server. The dual prediction model, however, is unable to predict data patterns with enough accuracy, which has the possibility to result in less than ideal energy savings. A butter Ant optimization in fuzzy dynamic trust-based RPL protocol proposed by [15] improves the security of data transmission. It offered scalable and safe medical data transfer. The protocol is made more complex by the addition of fuzzy logic, dynamic trust management, and optimization algorithms. Developed in [16], the optimized energy-efficient secure routing protocol reduces congestion of the network, offers safe data transfer, and chooses the network's best route. On the other hand, high network traffic resulting from improper routing will negatively affect system performance. In order to overcome this issue, the proposed work adopted a specialized routing protocol called Modified Gazelle Optimized Routing. This approach minimizes latency and maximizes throughput, facilitating continuous and expedited transfer of health data across the network. Although deep learning techniques will be integrated with blockchain technology to further enhance its potential, this provides a strong basis for secure healthcare solutions.

By producing a hash of each data point, [17] offered a CNN-based healthcare data security architecture that uses the blockchain method. This will notify all blockchain network users of any unauthorized data modifications or breaches in the medication supply. The CNN method has demonstrated its peak performance with varying data set sizes in this instance. Blockchain has scalability issues despite its benefits for security. The block chain size grows as the number of transactions rises, which possibly will have a consequence on the scalability of the system. In order to detect intrusions by improving security, the Blockchain-based African Buffalo (BbAB) system using an RNN model is developed in [18]. Its primary purpose is to accurately detect intrusions in cloud environments. Nonetheless, it is necessary to take into consideration an enhanced deep learning model that improves security performance and resolves the problem of data complexity in a cloud context. An intrusion detection system based on the BILSTM approach is presented by [19–20]. The condensed findings obtained from the performance of the misbehavior detection algorithms using the BILSTM method recommend that the algorithms are successful in identifying harmful events within the target healthcare system. But concerns about security and privacy still exist, particularly in situations where safety is at risk. Therefore, a DLT-trained RNN-BILSTM approach is implemented to ensure the data privacy and integrity of network nodes. The main goals of this work are as below,

- To offer a safe and tamper-resistant platform for storing and accessing sensitive healthcare data, thereby safeguarding patient privacy and confidentiality, the blockchain method is used.
- To find the shortest path for efficient data transfers within the blockchain network, a Modified Gazelle Optimized Routing approach is employed.
- To assure the data privacy and integrity of network nodes, a DLT-trained RNN-BILSTM approach is implemented.

p-ISSN: 2528-1682
e-ISSN: 2527-9165

2. PROPOSED METHODOLOGY

The healthcare system produces, distributes, stores, and uses a huge amount of data on a daily basis. Using blockchain technology to improve health record management reduces the complexity of the present, expensive healthcare system. It is crucial to have safe, secure, and scalable systems for sharing healthcare data in order to diagnose patients and collaborate on treatment decisions. Therefore, this paper proposes a DLT-trained RNN-BILSTM approach. Fig. 1 represents the proposed work's block diagram.

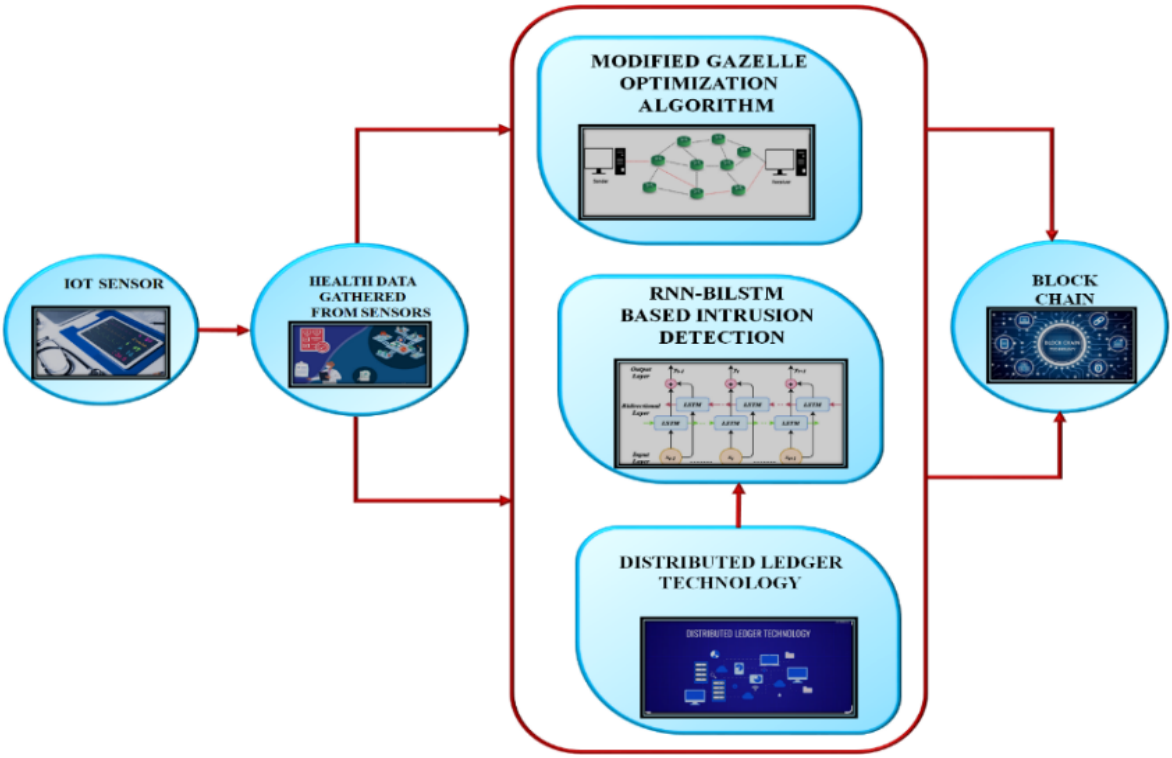

Figure 1. Block Diagram of Proposed Work

The health care data is collected from an IoT sensor, which acts as an input to a specialized routing protocol called Modified Gazelle Optimized Routing. This method is utilized to find the shortest path for efficient data transfer. It minimizes latency and maximizes throughput, facilitating continuous and expedited transfer of health data across the network. However, healthcare networks face security risks because of the sensitive nature of the data they handle, and this is overcome by using a DLT-trained RNN-BILSTM-based IDS. Here, the IDS enhances healthcare data security by identifying and mitigating potential threats, ensuring the integrity and confidentiality of patient information. The DLT-trained RNN-BILSTM-based IDS efficiently detects different types of attacks with high accuracy, including previously unknown threats, thereby ensuring the integrity and availability of healthcare data.

2.1. Modified Gazelle Optimized Routing Protocol for Finding the Shortest Path

The shortest path for effective data transfers within the blockchain network is found by using Modified Gazelle Optimization. This method reduces latency and increases throughput by using a specific routing protocol called Modified Gazelle Optimized Routing, which enables continuous and quick movement of health data throughout the network.

2.1.1. GOA Algorithm

The GOA algorithm's optimization process is split into 2 stages: Rummaging, which is known as the stage of exploitation, and eluding, when the hunter is found, which is named as the exploration stage. The gazelle's ability to avoid predators while foraging serves as the inspiration for this algorithm, which updates the candidate's solution.

2.1.1.1. Exploitation Stage

Gazelles peacefully foraging in the absence of hunters, and this procedure is predicated on the idea that each gazelle's location follows Brownian motion. The process for updating a gazelle's position is as follows:

$$x_i^{pl} = x_i + v.r_1.R_b(Elite - R_b \times x_i) \quad (1)$$

The locations of the i^{th} gazelle earlier and later, the initial position update phase are represented byx_i^{pl} andx_i; the gazelle's foraging speed is denoted by$v$; r_1 is a random number that occurs between 0 and 1; Elite denotes the optimal gazelle's position; and $R_b$is a Brownian motion's position vector that will be attained as

$$f_b(x, \mu, \sigma) = \frac{1}{\sqrt{2\pi\sigma}} \exp\left(-\frac{(x-\mu^2)}{2\sigma^2}\right) = \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{x^2}{2}\right) \quad (2)$$

In the above equation, $f_b(x, \mu, \sigma)$ denotes the Gaussian probability distribution function of the Brownian motion position vector R_b; the value of μ is 0and$\sigma^2 = 1$.

2.1.1.2. Exploration Stage

A gazelle rapidly swung its tail and beat its hooves to flee, and the hunter will pursue after spotting. The direction characteristic variable will be used to define it because both runs exhibit the signs of a mutation. The gazelle will opt to flee in one way if the number of iterations is odd, and in a different direction if the number of iterations is even. The position updates of some gazelles saw the Levy flight mode since they were the ones that initially located the hunter and led the response. The delayed response from the other part of the gazelle develops that it initially follows a Brownian motion pattern before transitioning to a Levy flight mode. At this stage, the gazelle's location update formula is as follows:

$$x_i^{p2.l} = x_i + v.\mu_g.r_2.R_1(Elite - R_l \times x_i) \quad (3)$$

$$x_i^{p2.2} = x_i + v.\mu_g.\ c_f.R_b(Elite - R_l \times x_i) \quad (4)$$

Where $x_{i,j}^{p2.1/2}$ denotes the location at thej^{th} the dimension of the i^{th} gazelle next to the 2 stage of location update, μ_g denotes directional characteristic variable; $r_2$is a random number, they are within the range of 0 and 1andc_f signifies the cumulative effect of the hunter, which is computed as follows:

$$c_f = \left(1 - \frac{m}{M}\right)^{2m/M} \quad (5)$$

Here $m\ and\ M$ are the present and maximum iteration numbers. If the gazelle effectively evades the chase of the hunter will be denoted as

$$x_i^{p2.3} = \begin{cases} x_i + c_f[l_b + r_3.(u_b - l_b)].Q\ if r' \le psrs \\ x_i + [psrs(1 - r_4) + r_4](x_{r1} - x_{r2})\ \ else \end{cases} \quad (6)$$

$$U = \begin{cases} 0, if\ r_4 < 0.34 \\ 1,\ \ else \end{cases} \quad (7)$$

Here, u_b and l_b are the higher and lower location bounds of the gazelle individual, respectively; $r_{3,4}$ are two random numbers,, $r_{3,4} \in [0, 1]$; $psrs$ denotes the $F(x_i^{p2})$ denotes the rate of escape, gotten as 0.34; and a binary vector is indicated as Q contained the random numbers in 0 and 1. However, the GOA often exhibits premature convergence, becoming ensnared in local optima. This limitation impedes

p-ISSN: 2528-1682
e-ISSN: 2527-9165

thorough exploration of the solution space, thus hindering the discovery of global optima. So, this paper uses a Modified Gazelle Optimization Algorithm, which is utilized to find the shortest path.

2.1.2. Modified Gazelle Optimization Algorithm

It is mainly used for routing purposes, such as finding the shortest path for efficient data transfers within the blockchain network.

2.1.2.1. Logistic Mapping Initialization

This study incorporates logistic mapping into an initialization procedure of the GOA algorithm to symmetrically improve the distribution of the primary solution set in terms of both uniformity and unpredictability. The definition of the logistic map is as follows:

$$x_{i+1} = x_i \times \varphi \times (1 - x_i) \tag{8}$$

Here, ψ denotes the logistic coefficient that is within the range 0 and 4.

2.1.2.2. Gaussian Mutation Coefficient and Logarithmic Inertia Weight

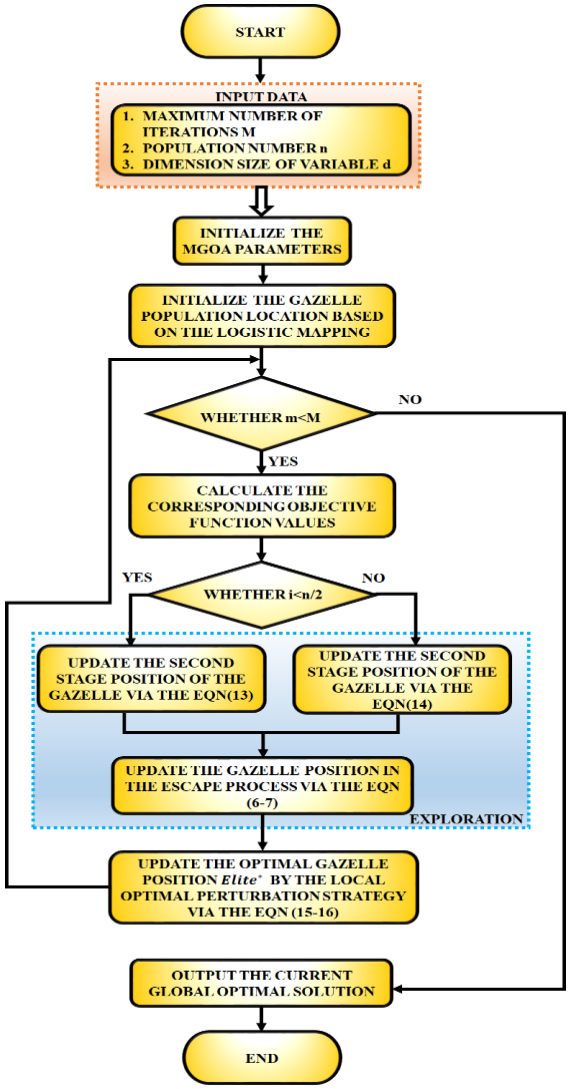

Figure 2. Flowchart of Modified Gazelle Optimization Algorithm.

Incorporating the Gaussian mutation coefficient and logarithmic inertia weight into the location modernize formula of the gazelle during the 1st and 2nd phases of the GOA algorithm will augment the algorithm's global search capability throughout an iterative process.

$$\omega = ({}^{m}/_{M}) \times (lgw_{lgw_{min}max} - lgw_{max}) \tag{9}$$

$$\varepsilon = r_5 \times \left(1 - \left(\frac{m}{M}\right)^2\right) \tag{10}$$

$$k = \sqrt{2\sigma^2 \log\left(\frac{1}{1-\varepsilon}\right) \times \cos(2\pi r_6)} \tag{11}$$

Where ω represents the logarithmic inertia weight; ω_{max}andω_{min}denote the maximum and minimum values; ε is a random variable associated with the present iteration number; k signifies the Gaussian mutation coefficient; and $r_{5,6}$ are two random numbers within the range of 0 and 1 . Figure 2 displays the flowchart of the modified gazelle optimization algorithm. The enhanced location update formula for the gazelle individual during the 1st and 2nd steps is given by:

$$x_i^{pl} = x_i + v.r_1.R_b(\omega \times Elite - R_b \times x_i) \tag{12}$$

$$x_i^{p2.l} = x_i + v.\mu_g.r_2.R_1(k \times Elite - R_l \times x_i) \tag{13}$$

$$x_i^{p2.2} = x_i + v.\mu_g.\ c_f.R_b(k \times Elite - R_l \times x_i) \tag{14}$$

2.1.2.3. Local Optimal Perturbation Strategy

An optimal individual's local perturbation process in its neighborhood is defined as

$$Elite' = \begin{cases} Elite + r_5.Elite, r_5 < 0.5 \\ Elite, r_5 \geq 0.5 \end{cases} \tag{15}$$

Here r_5 is a random number and that belongs to [0, 1]; $Elite$ and$Elite'$ denote the location of an optimal individual earlier and later optimization.

$$Elite* = \begin{cases} Elite', F(Elite') < F(Elite) \\ Elite.F(Elite') \geq F(Elite) \end{cases} \tag{16}$$

Here $Elite*$indicates the updated location of the optimal individual; $F(Elite)$ and $F(Elite')$, denote the values of the objective function earlier and later the updating. This approach minimizes latency and maximizes throughput, facilitating continuous and expedited transfer of health data across the network. The following methods are utilized to assure the data confidentiality and integrity of network nodes.

2.2. Distributed Ledger Technology (DLT) Trained RNN-BILSTM-Based Intrusion Detection System (IDS)

To assure the data privacy and integrity of network nodes, a DLT-trained RNN-BILSTM approach is implemented. Blockchain's DLT facilitates safe transmission of patient medical records, reinforces healthcare data defenses, and controls the supply chain of medicine.

2.2.1. Distributed Ledger Technology

DLT holds significant promise for rapid adoption within the healthcare sector as a digital service. Essentially, a distributed ledger functions as a decentralized database, managed through a consensus protocol executed by nodes within a peer-to-peer network. Unlike traditional systems, this protocol eliminates the need for a central administrator, as all network participants collaborate to uphold the database's integrity. This decentralization permits individuals by granting them greater control over their data, free from reliance on a central controller.

p-ISSN: 2528-1682
e-ISSN: 2527-9165

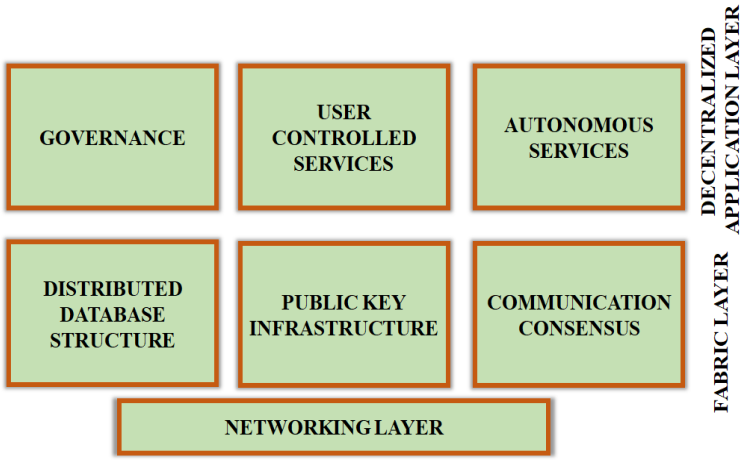

Figure 3. Distributed ledger system's layers.

DLTs are structured into two foundational layers, illustrated in Fig. 3. A first layer, known as the fabric layer, encompasses a code base governing communication, consensus mechanisms, public key infrastructure, and database organization. A second layer is the application layer, where logic resides, and where anyone can innovate by creating decentralized applications that operate atop the fabric layer. It's crucial to recognize that those who maintain and conserve a fabric layer wield control over the system's core functionalities, implying a degree of centralization in this technology. Nevertheless, decentralized governance models exist within the application layer, empowering network contributors to influence future updates to the fabric layer. While distributed ledgers permit any peer to generate new transactions and access the shared database, attempts to tamper with past transactions are swiftly identified by authentic peers. This resilience against malicious alterations after transaction acceptance by all network participants renders it challenging for adversaries to manipulate historical data stored within the distributed ledger. Modern cryptographic primitives like distributed consensus procedures built into the fabric layer and one-way hash functions are responsible for the creation of this trustless environment. Every transaction that is added to a distributed ledger is uniquely and readily verifiably related to previous transactions using cryptography. Due to the ledger's ability to spread changes to previously recorded transactions, these relationships provide chronology and peer trust. It is possible to share databases in a peer-to-peer network without requiring mutual trust between users, thanks to specialized distributed consensus methods. Cryptographic currency and smart contracts are two examples of innovative decentralized applications made possible by the trustless distribution of databases among several peers. The trade-off between transaction finality and latency exists in current protocols, despite the potential of this developing technology.

A transaction on the Bitcoin network is final. It is customary to wait 6 blocks to be included in the lengthiest chain. This translates to a wait time of roughly one hour. Applications that need low latency and value exchange are dependent on the payer not double-spending and guarantee that their transactions will be completed in a timely manner. The existing incentive structures that facilitate the viral propagation of these protocols employ computing resources inefficiently and limit the network's transaction rate. DLT solves health care systems' interoperability issues, enabling safe and effective data interchange. Due to DLT's transparency and immutability, data security is guaranteed. Better performance is ensured by training DLT with RNN-BILSTM, which detects various kinds of attacks. To ensure better performance, DLT is trained with RNN-BILSTM that finds different types of attacks.

2.2.2. RNN-BILSTM-Based IDS

RNN-BILSTM trained by DLT is utilized to safeguard the integrity and confidentiality of network nodes' data. Artificial neural networks known as RNNs allow for the cycling of the effects of one node's output on the following input of other nodes. Its behavior exhibits temporal dynamics as a result. As a

descendant of feed-forward neural networks, RNNs will interpret sequences of inputs of different lengths by remembering internal states. In RNNs, all input vector components share approximately equal weights, unlike in feed-forward NNs, where each component has its own weight. RNNs often outperform conventional methods because they consolidate the weights of positions of the multiple input vectors into a single vector, allowing them to process varying-length sequences using the same method by reusing these weights. This reduction in the network-learning parameters (weights) is an extra advantage. Additionally, the outputs passed on to the succeeding stage are calculated using both the numerous data points and the input vector from the preceding step, typically another vector. "Units" represent the formulas employed to develop the middle results. Hence, in the most basic form of an RNN, the following relationship, represented by Equations 17 and 18, defines a block:

$$O^{<t>} = f_1(W_{oo}O^{<t-1>} + W_{ox}\, x^{<t>} + b_o) \quad (17)$$

$$\hat{y}^{<t>} = f_2(W_{yo}O^{<t>} + b_y) \quad (18)$$

Here, $x^{<t>}$ represents an input vector sequence, where t indicates the iteration at which the relations of the recurrent are calculated. The functionsf_1 and $f_2$denote activation functions. $W_{oo,}W_{ox}\ W_{yo}, b_o\ and\ b_y are$ Indicates the weight matrices and biases. LSTM is a unit of RNNs designed to mitigate the vanishing gradients problem. Additionally, this architecture excels at preserving long variety connections by understanding the relationships between values at the sequence's beginning and end.

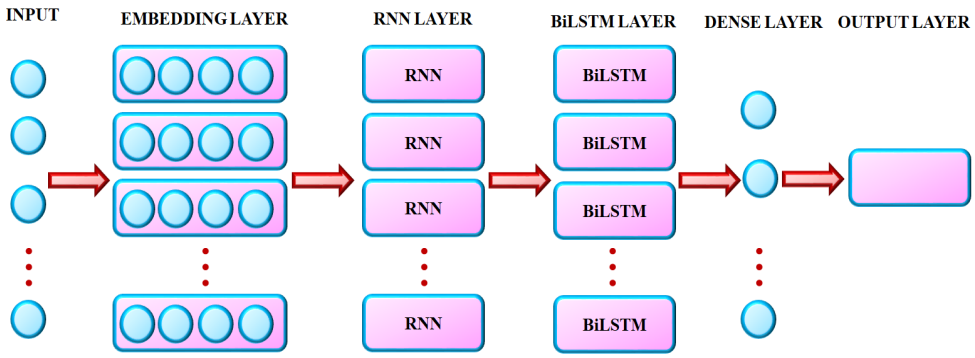

Figure 4. The RNN-BILSTM model architecture

In the LSTM model, these functionalities manifest as gates, comprising 3 different ranges: The forget gate controls the transfer of data from 1 memory cell to another, controlling the retention or dismissal of information. The update gate, also known as the memory cell's update input, determines whether the cell will be updated. It also governs the flow of data from a potential new memory cell to the present one. The output gate dictates the value of the next hidden state. This study introduces the integration of RNN and BILSTM for detecting different types of attacks. The network architecture includes 5 layers: an input layer sequence, an RNN layer with 100 hidden units, a BILSTM layer with 200 hidden units, a Fully Connected (FC) layer, a Softmax layer, and an output classification layer. A kind of RNN structure, the binary LSTM network, has demonstrated reliability and effectiveness in simulating sequences with prolonged dependencies for various purposes, including time-dependent research scenarios. After the RNN module, a BILSTM layer was incorporated to accommodate the time-sequenced nature of collected signals, where the current state heavily relies on past contexts. Addressing this issue, the BILSTM model proves to be a highly effective tool. It boasts several self-parameterized regulating gates within its memory cell, facilitating state information manipulation, as illustrated in Figure 4. The opening of these gates would unleash the cell's full informational potential. To summarize, the failure of the previous cell's process stemmed from the neglect of the forget gate, potentially resulting in the neglect of preceding data. The output gate autonomously determines whether to transmit the latest cell output and the ultimate state. Additionally, to mitigate over-fitting, two dropout layers positioned beneath the ReLU activation function, alongside a BILSTM layer, are employed. These dropout layers

p-ISSN: 2528-1682
e-ISSN: 2527-9165

effectively combat overfitting while aiding in minimizing generalization error, particularly with the expansion of NN layers. Given the vast amounts of health care data, effective intrusion detection is imperative to safeguard sensitive information before any attacks occur. This paper proposes an RNN-BILSTM-based IDS for efficiently detecting various attack types. While RNN-based intrusion detection models automate local feature extraction, they fall short in capturing temporal correlations within intrusion data. In contrast, BILSTM-based intrusion detection models excel in identifying persistent attack behaviors by extracting bidirectional temporal features from intrusion data. Therefore, combining the advantages of RNN and BILSTM, this paper uses an intrusion detection model based on RNN-BILSTM, which effectively finds various attacks present in the healthcare management system.

3. RESULTS AND DISCUSSION

By adopting a Modified Gazelle Optimized Routing, a specialized routing protocol that minimizes latency and maximizes throughput, it facilitates continuous and expedited transfer of health data across the network. To assure the data confidentiality and integrity of network nodes, a DLT-trained RNN-BILSTM approach is implemented. The proposed RNN-BILSTM-based IDS efficiently detects different types of attacks with high accuracy.

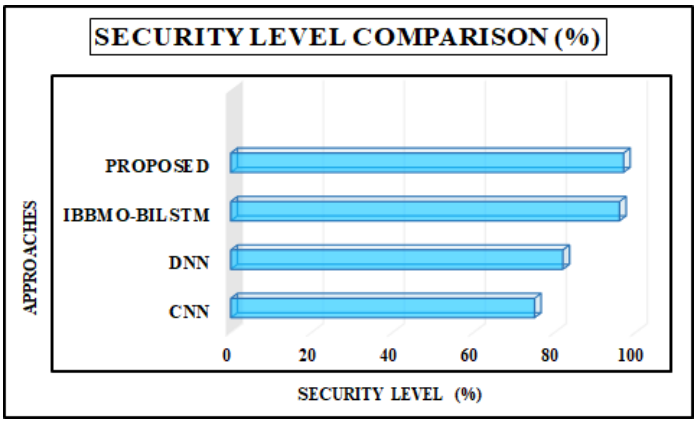

Figure 5. Security level comparison

Figure 5 depicts the security level comparison of CNN [23], DNN [24], IBBMO-BILSTM [25], and RNN-BILSTM methods. The proposed work has the highest security level of 97% which is better than other methods.

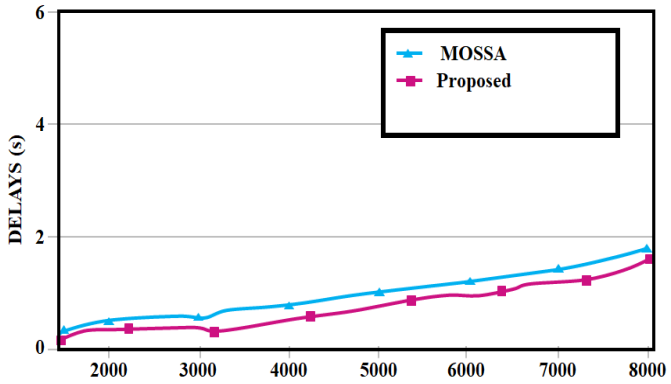

Figure 6. Delay Performance

Figure 6 displays the delay performance of the Multi-Objective Squirrel Search Optimization Algorithm (MOSSA) and the Modified Gazelle Optimization algorithm. The proposed algorithm achieves the lowest delay than the MOSSA [26].

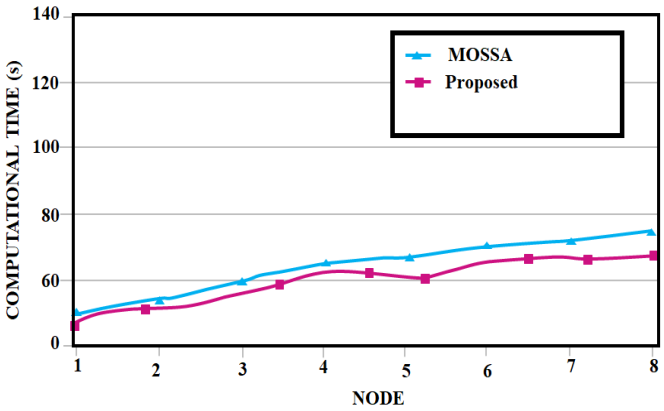

Figure 7. Computational time Performance

Figure 7 illustrates the computational time performance of MOSSA and the Modified Gazelle Optimization algorithm. The proposed algorithm attains the lowest computational time than the MOSSOA [26].

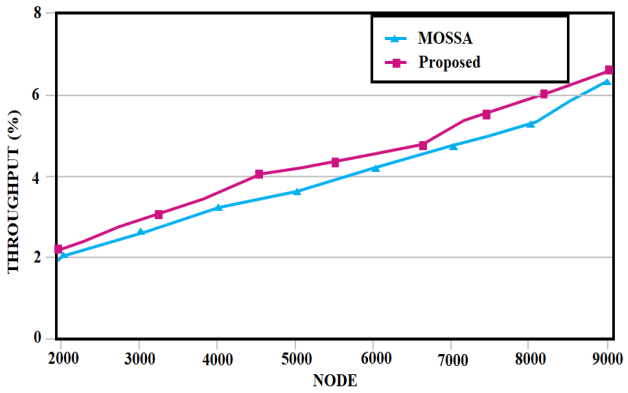

Figure 8. Performance of throughput.

The proposed algorithm attains the higher throughput than the MOSSA [26]. Figure 8 illustrates the throughput performance of MOSSA and the Modified Gazelle Optimization algorithm.

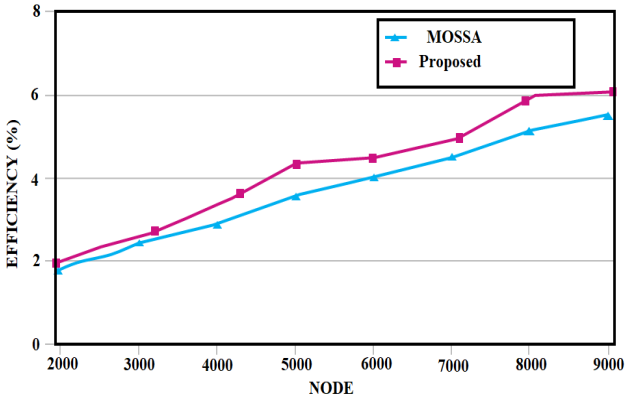

Figure 9. Performance of efficiency.

p-ISSN: 2528-1682
e-ISSN: 2527-9165

Figure 9 represents the efficiency performance of MOSSA [26] and the Modified Gazelle Optimization algorithm. The proposed algorithm attains higher efficiency than the MOSSOA.

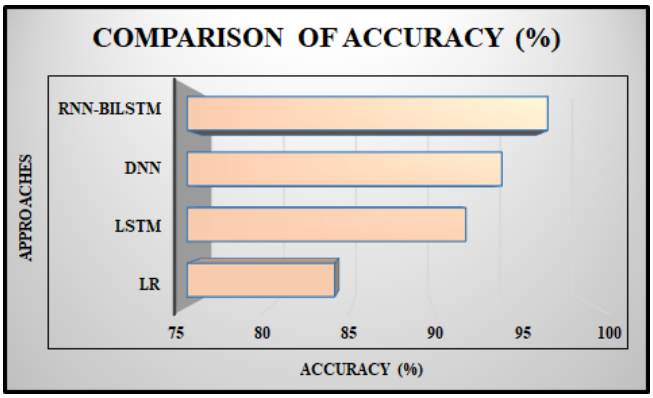

Figure 10. Accuracy comparison.

Figure 10 depicts the accuracy comparison with different methods like LR [21], LSTM [22], DNN [19], and RNN-BILSTM. The RNN-BILSTM attains an accuracy of 97 % which is better than other methods.

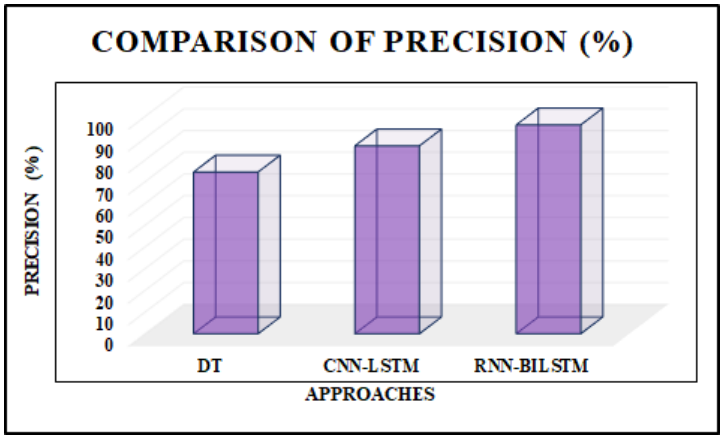

Figure 11. Comparison of precision.

Figure 11 shows the comparison of precision for some methods such as DT [19], CNN-LSTM [22] and RNN-BILSTM. The proposed RNN-BILSTM outperformed other methods with a precision of 96.1%.

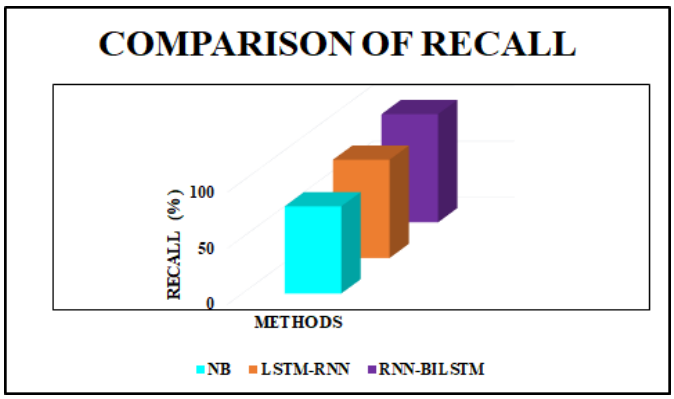

Figure 12. Comparison of Recall.

Figure 12 shows the recall comparison for some methods like NB [19], LSTM-RNN [22] and the proposed RNN-BILSTM attains the recall of 96.4% that is better than other methods.

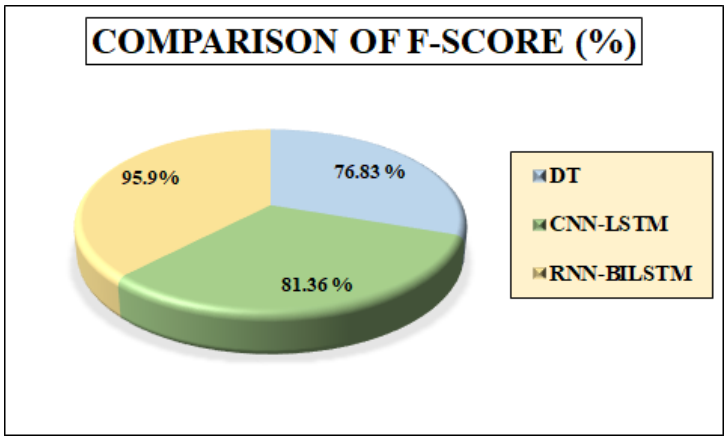

Figure 13. Comparison of F-score

Figure 13 displays the comparison of F-score with methods like DT [19], CNN-LSTM [22], and the proposed RNN-BILSTM achieves the F-score value of 95.9% which is better than other methods.

Table 1. Analysis of the detection rate

Appraoches /Attacks	Cnn-Bilstm	Proposed
DOS	27%	30 %
Fuzzers	85 %	88 %
Shell code	92 %	93 %

The analysis of the detection rate for CNN-BILSTM [27] and the developed approach is shown in Table 1. In the Denial of Service (DoS) attacks, the developed approach has a better detection rate of 30 % than CNN-BILSTM (27%). In Fuzzers, the developed model attains 88% accuracy, surpassing CNN-BILSTM (85%). Also, for the Shell code, the developed model has a higher rate of 93% than CNN-BILSTM (92 %), demonstrating reliable performance over attack types.

Table 2. Analysis of Standard Deviation

Approaches	Standard Deviation
GOA [28]	3.8054×10^{-50}
Proposed	3.512×10^{-50}

The analysis with GOA and the developed approach in terms of standard deviation is shown in Table 2. The better Standard deviation of 3.512×10^{-50} result is attained by the developed approach than GOA. The incorporation of blockchain and deep learning, utilizing modified Gazelle optimization and DLT-trained RNN-BILSTM, is developed to minimize computational overhead on IoT by offloading complex tasks to distributed edge nodes and optimizing routing paths. The modified Gazelle optimization assures low latency and energy-efficient data transfer. The training of RNN-BILSTM on the DLT structure enables the IoT devices to perform only inference operations. It allows secure, real-time data processing with minimal resource consumption, appropriate for resource-constrained IoT environments.

4. CONCLUSION

This paper proposes a Modified Gazelle Optimization that enables the determination of the shortest path for efficient data transfers within the blockchain network. By employing a decentralized and immutable ledger, blockchain provides a secure and tamper-resistant platform for storing and accessing sensitive data of healthcare, thereby safeguarding patient privacy and confidentiality. To safeguard the data integrity and privacy of network nodes, a DLT-trained RNN-BILSTM approach is

implemented. This advanced DL technique enhances the security and reliability of the network by detecting and preventing unauthorized access and tampering attempts. The proposed RNN-BILSTM-based IDS efficiently detects different types of attacks including previously unknown threats, thereby warranting the integrity and availability of healthcare data. The comparative analysis is done with conventional methods that prove the proposed method is much better than other methods. With a 97% accuracy rate, the research's findings confirm the effectiveness and consistency of the proposed approach in improving the security, efficiency, and performance matrix, protecting the confidentiality and integrity of medical records.

REFERENCES

[1] A. A. Abdellatif, A. Z. Al-Marridi, A. Mohamed, A. Erbad, C. F. Chiasserini and A. Refaey, "ssHealth: toward secure, blockchain-enabled healthcare systems," IEEE Network, vol. 34, no. 4, pp. 312-319, April 2020, doi: https://doi.org/10.1109/MNET.011.1900553.

[2] A. Ali, H. Ali, A. Saeed, A. A. Khan, T. T. Tin, M. Assam, Y. Y. Ghadi and H. G. Mohamed, "Blockchain-Powered Healthcare Systems: Enhancing Scalability and Security with Hybrid Deep Learning," Sensors, vol. 23, no. 18, pp. 7740, September 2023, doi: https://doi.org/10.3390/s23187740.

[3] M. Younis, W. Lalouani, N. Lasla, L. Emokpae and M. Abdallah "Blockchain-enabled and data-driven smart healthcare solution for secure and privacy-preserving data access," IEEE Systems Journal, vol. 16, no. 3, pp. 3746-3757, July 2021, doi: https://doi.org/10.1109/JSYST.2021.3092519.

[4] K. Azbeg, O. Ouchetto and S. J. Andaloussi, "BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security," Egyptian informatics journal, vol. 23, no. 2, pp. 329-343, July 2022, doi: https://doi.org/10.1016/j.eij.2022.02.004.

[5] R. Bhan, R. Pamula, P. Faruki and J. Gajrani, "Blockchain-enabled secure and efficient data sharing scheme for trust management in healthcare smartphone network," The Journal of Supercomputing, vol. 79, no. 14, pp. 16233-16274, September 2023, doi: https://doi.org/10.1007/s11227-023-05272-6.

[6] S. Tatineni, "Integrating Ai, Blockchain and Cloud Technologies for Data Management in Healthcare," Journal of Computer Engineering and Technology (JCET), vol. 5, no. 01, January 2022.

[7] R. G. Sonkamble, A. M. Bongale, S. Phansalkar, A. Sharma and S. Rajput, "Secure data transmission of electronic health records using blockchain technology," Electronics, vol. 12, no. 4, pp. 1015, February 2023, doi: https://doi.org/10.3390/electronics12041015.

[8] M. S. Islam, M. A. Bin Ameedeen, M. A. Rahman, H. Ajra and Z. B. Ismail "Healthcare-chain: blockchain-enabled decentralized trustworthy system in healthcare management industry 4.0 with cyber safeguard," Computers, vol. 12, no. 2, pp. 46, February 2023, doi: https://doi.org/10.3390/computers12020046.

[9] N. Sammeta and L. Parthiban "Hyperledger blockchain enabled secure medical record management with deep learning-based diagnosis model," Complex & Intelligent Systems, vol. 8, no. 1, pp. 625-640, February 2022, doi: https://doi.org/10.1007/s40747-021-00549-w.

[10] E. P. Adeghe, C. A. Okolo, and O. T. Ojeyinka, "Evaluating the impact of blockchain technology in healthcare data management: A review of security, privacy, and patient outcomes," vol. 10, no. 2, pp. 013-20, May 2024, doi: https://doi.org/10.53022/oarjst.2024.10.2.0044.

[11] A. A. Khan, A. A. Laghari, M. Shafiq, O. Cheikhrouhou, W. Alhakami, H. Hamam, and Z. A. Shaikh "Healthcare ledger management: A blockchain and machine learning-enabled novel and secure architecture for medical industry," Hum. Cent. Comput. Inf. Sci, vol. 12, pp. 55, November 2022, doi: https://doi.org/10.22967/HCIS.2022.12.055.

[12] A. A. Bahattab, A. Trad, and H. Youssef, "PEERP: A priority-based energy-efficient routing protocol for reliable data transmission in healthcare using the IoT," Procedia Computer Science, vol. 175, pp. 373-378, January 2020, doi: https://doi.org/10.1016/j.procs.2020.07.053.

[13] N. Ahmad, M. D. Awan, M. S. Hayat Khiyal, M. I. Babar, A. Abdelmaboud, H. A. Ibrahim, and N. O. Hamed, "Improved QoS aware routing protocol (IM-QRP) for WBAN based healthcare monitoring system," IEEE Access, vol.10, pp.121864-121885, November 2022, doi: https://doi.org/10.1109/ACCESS.2022.3223085.

[14] F. A. Almalki, S. Ben Othman, F. A. Almalki, and H. Sakli, "EERP-DPM: Energy efficient routing protocol using dual prediction model for healthcare using IoT," Journal of Healthcare Engineering, vol. 2021, pp. 1-15, May 2021, doi: https://doi.org/10.1155/2021/9988038.

[15] E. Refaee, S. Parveen, K. M. J. Begum, F. Parveen, M. C. Raja, S. K. Gupta, and S. Krishnan, "Secure and scalable healthcare data transmission in IoT based on optimized routing protocols for mobile computing applications," Wireless Communications and Mobile Computing. pp. 1-12, June 2022, doi: https://doi.org/10.1155/2022/5665408.

[16] R. Singla, N. Kaur, D. Koundal, S. A. Lashari, S. Bhatia, and M. K. I. Rahmani, "Optimized energy efficient secure routing protocol for wireless body area network," IEEE Access, vol. 9, pp. 116745-116759, August 2021, doi: https://doi.org/10.1109/ACCESS.2021.3105600.

[17] A. B. Tello, J. Xing, A. L. Patil, L. P. Patil, and S. Sayyad, "Blockchain Technologies in Healthcare System for Real Time Applications Using IoT and Deep Learning Techniques," International Journal of Communication Networks and Information Security, vol. 14, no. 3, pp. 257-268, December 2022.

[18] V. Saravanan, M. Madiajagan, S. M. Rafee, P. Sanju, T. B. Rehman, and B. Pattanaik, "IoT-based blockchain intrusion detection using optimized recurrent neural network," Multimedia Tools and Applications, vol. 83, no. 11, pp. 31505-31526, March 2024, doi: https://doi.org/10.1007/s11042-023-16662-6.

[19] P. Kumar, R. Kumar, G. P. Gupta, R. Tripathi, A. Jolfaei, and A. N. Islam, "A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system," Journal of Parallel and Distributed Computing, vol. 172, pp. 69-83, February 2023, doi: https://doi.org/10.1016/j.jpdc.2022.10.002.

[20] S. Rahmadika, P. V. Astillo, G. Choudhary, D. G. Duguma, V. Sharma, and I. You, "Blockchain-based privacy preservation scheme for misbehavior detection in lightweight IoMT devices," IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 710-721, June 2022, doi: https://doi.org/10.1109/JBHI.2022.3187037.

[21] T. S. Pooja, and P. Shrinivasacharya, "Evaluating neural networks using Bi-Directional LSTM for network IDS (intrusion detection systems) in cyber security," Global Transitions Proceedings, vol. 2, no. 2, pp. 448-454, November 2021, doi: https://doi.org/10.1016/j.gltp.2021.08.017.

[22] A. Aldallal, "Toward efficient intrusion detection system using hybrid deep learning approach," Symmetry, vol. 14, no. 9, pp. 1916, September 2022, doi: https://doi.org/10.3390/sym14091916.

[23] P. Qi, D. Chiaro, F. Giampaolo, and F. Piccialli, "A blockchain-based secure Internet of medical things framework for stress detection," Information Sciences, vol. 628, pp. 377-390, May 2023, doi: https://doi.org/10.3390/sym14091916.

[24] S. K. Somayaji, M. Alazab, M. K. Manoj, A. Bucchiarone, C. L. Chowdhary, and T. R. Gadekallu "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, December 2020, doi: https://doi.org/10.1109/GCWkshps50303.2020.9367413.

[25] H. Singh, Z. Ahmed, M. D. Khare, and J. Bhuvana, "An IoT and blockchain-based secure medical care framework using deep learning and nature-inspired algorithms," International Journal of Intelligent Systems and Applications in Engineering, vol. 11, no. 8s, pp. 183-191, July 2023.

[26] B. Jaishankar, S. Vishwakarma, P. Mohan, A. K. S. Pundir, I. Patel, and N. Arulkumar, "Blockchain for securing healthcare data using squirrel search optimization algorithm," Intelligent Automation & Soft Computing, vol. 32, no. 3, pp. 1815-1829, January 2022, doi: http://dx.doi.org/10.32604/iasc.2022.021822.

[27] W. Dai, X. Li, W. Ji, and S. He, "Network intrusion detection method based on CNN, BiLSTM, and attention mechanism," IEEE Access, vol. 12, pp. 53099 - 53111, April 2024, doi: https://doi.org/10.1109/ACCESS.2024.3384528.

[28] D. Wu, L. Wu, T. Wen, and L. Li, "Microgrid operation optimization method considering power-to-gas equipment: An improved gazelle optimization algorithm," Symmetry, vol. 16, no. 1, pp. 83, January 2024, doi: https://doi.org/10.3390/sym1601