An Optimized Deep Learning Based Malicious Nodes Detection in Intelligent Sensor-Based Systems Using Blockchain

Swathi Darla [1,2,*] and C. Naveena [2]

[1] Department of Information Science and Engineering, R. V. Institute of Technology and Management, Bangalore, India
[2] Department of Computer Science and Engineering, SJB Institute of Technology, Bangalore, India;
Email: naveena.cse@gmail.com (C.N.)
*Correspondence: swathidarla.rvitm@rvei.edu.in (S.D.)

***Abstract*—In this research work, a blockchain-based secure routing model is proposed for Internet of Sensor Things (IoST), with the assistance acquired from deep learning-based hybrid meta-heuristic optimization model. The proposed model includes three major phases: (a) optimal cluster head selection, (b) lightweight blockchain-based registration and authentication mechanism, (c) optimized deep learning based malicious node identification and (d) optimal path identification. Initially, the network is constructed with N number of nodes. Among those nodes certain count of nodes is selected as optimal cluster head based on the two-fold objectives (energy consumption and delay) based hybrid optimization model. The proposed Chimp social incentive-based Mutated Poor Rich Optimization (CMPRO) Algorithm is the conceptual amalgamation of the standard Chimp Optimization Algorithm (ChOA) and Poor and Rich Optimization (PRO) approach. Moreover, blockchain is deployed on the optimal CHs and base station because they have sufficient storage and computational resources. Subsequently, a lightweight blockchain-based registration and authentication mechanism is undergone. After the authentication of the network, the presence of malicious nodes in the network is detected using the new Optimized Deep Belief Network. To enhance the detection accuracy of the model, the hidden layers of Deep Belief Network (DBN) is optimized using the new hybrid optimization model (CMPRO). After the detection of malicious nodes, the source node selects the shortest path to the destination and performs secure routing in the absence of malicious node. In the proposed model, the optimal path for routing the data is identified using the Dijkstra algorithm. As a whole the network becomes secured. Finally, the performance of the model is validated to manifest its efficiency over the existing models.**

***Keywords*—blockchain, security, malicious node detection, deep belief network, hybrid optimization model, Internet of Things (IoT), Wireless Sensor Networks (WSN)**

I. Introduction

IoT has become a significant force in advancing economic and social development as a result of the Internet's and perceptual technology's rapid development [1]. Wireless Sensor Networks (WSN) play a crucial role in advancing the development of IoT, which has significant practical significance and research value. WSNs are the key technology in the IoT architecture [2]. Sensing nodes are a collection of small, self-acting devices that make up a WSN. A computing device with memory, a battery, a processor, a transceiver, and a sensing device is known as a sensing node [3]. Sink nodes are technical nodes found in sensor networks that process and store the data brought together by the network. In the event that two nodes are not within each other's transmission range, communication takes place over a number of hops [4]. Wireless sensor networks are able to gather information from the surroundings in which they are set up. The sensor nodes frequently process the data first, after which it is frequently sent via unsecure channels to the sink node for additional processing [5]. Environmental monitoring, infrastructure management, public safety, healthcare, home and office security, transportation, and battlefield surveillance are a few of the applications for sensor networks that are foreseen. One can attack a WSN in a variety of ways [6]. For instance, it is possible to spoof a message's various fields while it is in transit so that the recipient receives a change version of the original message [7]. A node's hardware and/or software can also be modified in order to change how it behaves. Different attack types would call for various countermeasures [8]. The networks experience well-known problems as a result of their deployment in harsh and by oneself environments, such as the possibility of attacks by compromising the sensor nodes, which contain very sensitive data like Identification (ID) and location [9, 10]. The credentials are worn for cypher text generation during various cryptographic operations like encryption and decryption. However, by physically accessing the nodes, these credentials are abused. As a result, various solutions to the problem were tacit. Place the data on a central server that can maintain the records secretly and securely using a variety of cryptographic methods [11]. Furthermore, since the systems are governed by a single central authority, they are vulnerable to manipulation, which can undermine public trust.

The major contribution of this research work is:

Manuscript received January 2, 2023; revised March 4, 2023; accepted April 17, 2023; published October 8, 2023.

- To select the Optimal Cluster Head (OCH) based on the new two-fold objective-based hybrid optimization model.
- The proposed hybrid optimization model referred as Chimp social incentive-based Mutated Poor Rich Optimization Algorithm (CMPRO) is the conceptual amalgamation of the new standard Chimp Optimization Algorithm (ChOA) and Poor and Rich Optimization (PRO) approach.
- To identify the malicious nodes in the network using the optimized Deep Belief Network (DBN) model.
- To optimize the hidden layers of DBN using the new CMPRO model.

The rest of this paper is organized as: Section II manifest the literature works undergone in the subject. Section III provides information on the proposed secured network construction model. The results acquired by the proposed model is discussed clearly in Section IV. Finally, this paper is concluded in Section V.

II. Literature Review

A. Review

In 2019, She *et al.* [12] had presented a Blockchain Trust Mode (BTM) for wireless sensor networks' detection of malicious nodes. First, provided the complete trust model framework. The blockchain data structure used to identify malicious nodes is then built. In addition, the poll consensus results are recorded in the blockchain distributed, purview the detection of malicious nodes in 3D space by dint of the blockchain smart contract and the quadrilateral measurement localization method of the WSNs. The simulation results demonstrate that the model was capable of accurately determine malicious nodes in WSNs and safeguard the process's traceability.

In 2021, Sivaganesan *et al.* [13] had proposed a data driven trust mechanism based on blockchain as a decentralised and energy-efficient solution for internal attack detection in IoT powered WSNs. When compared to the current solutions, the proposed model reduces the message overhead under grey and black hole attack scenarios. The time it takes to find malicious nodes was also significantly shortened in both grey hole and black hole attacks. The enhancement of these factors results in a significant increase in network lifetime.

In 2021, Sajid *et al.* [14] had presented that Blockchain was used to exploit ML methods in order to increase network security. The unauthenticated nodes, which can be dangerous for the network, are first registered. The nodes involved in the routing process are registered after blockchain. It also stores the routing data that was produced over the routing process. Additionally, a Proof-of-Authority (PoA) consensus mechanism was utilised because Proof of Work (PoW) requires more computational power to validate the transactions.

In 2020, Tariq *et al.* [15] had offered a multi-mobile code-driven blockchain-based energy-efficient decentralised trust mechanism for pinpoint internal attacks in sensor node-powered IoT. The outcomes demonstrate that the suggested solution performs better than the alternatives.

Wu *et al.* [16] had developed and examined a Blockchain-Based approach called BBTM to manage trust in IoT systems with limited resources. To handle the trust assessment process between sensor nodes, it makes use of blockchain. The BBTM client layer and Blockchain layer are the two components that make up BBTM. The effectiveness of BBTM for trust computation was demonstrated while also keep the desired trust accuracy, convergence, and attack resistance. With regard to important design parameters, this paper performs a sensitivity analysis of BBTM performance. BBTM is compared to CATrust and CTM, and then, finally, it also does it. The experiments also assess the effectiveness of the blockchain network. The efficacy of the suggested method was demonstrated by experimental results.

B. Problem Statement

The external malicious nodes that snoop on communication channels and take personal information for their own gain pose a threat to the Internet of Sensor Things (IoST) nodes. Additionally, the nodes engage in malicious behaviour while the network is routing data and launch the gray hole attack. The authors in suggest a model to achieve authentication in the IoST that consists of two blockchains, encryption techniques, and digital signatures in order to address the problem. However, using two blockchains adds extra communication and processing costs. Ramezan and Leung [17] also use blockchain to solve the problem of a single point of failure and identify malicious activity using Merkle trees. Hong [18] uses a secure hashing algorithm based on a blockchain for node authentication. The algorithm aids in the network's MN detection. Haseeb and Islam *et al.* [19] suggest a blockchain-based secure data storage system. However, in contrast to other centralised storage platforms, blockchain-based data storage is more expensive. To find the secure route, trust aware localised routing is used in [20]. Additionally, a blockchain-based authentication system is suggested. However, the forwarding nodes use a lot of energy when sending the data packets without taking the optimal route into account. Xu and Ren *et al.* [21] proposes a blockchain-based nonrepudiation service provisioning scheme that prevents both service provider and client denial. The proposed scheme's use of homomorphic hashing for service verification, which has a high computational cost, is the cause for the decline of the proposed model. To overcome such drawbacks, a new optimized deep learning based malicious node detection model is introduced in this research work. Table I describes the abbreviations used in this paper.

TABLE I. Nomenclature

Abbreviation	Definition
DBN	Deep Belief Network
PoA	Proof of Authority
PoW	Proof of Work
DNN	Deep Neural Network
RBM	Restricted Boltzmann Machine
DBM	Deep Boltzmann Machines
PRO	Poor and Rich Optimization
ChOA	Chimp Optimization Algorithm

III. Proposed Model

With the aid of a hybrid meta-heuristic optimization model based on deep learning, a blockchain-based secure routing model for the Internet of Sensor Things (IoST) is proposed in this research. The proposed model has three main phases: (a) selecting the best cluster head; (b) using a light-weight blockchain-based registration and authentication mechanism; (c) identifying malicious nodes using deep learning; and (d) choosing the optimal path.

Optimal cluster head selection: The network is first built with N nodes. One of these nodes is chosen to serve as the cluster leader. This hybrid optimization model with two objectives (energy consumption and delay) is used to choose the best cluster head. The traditional Chimp Optimization Algorithm (ChOA) and the Poor and Rich Optimization (PRO) method are conceptually combined in the suggested hybrid optimization model (Chimp social incentive-based Mutated Poor Rich Optimization Algorithm (CMPRO)). Furthermore, the best CHs and base stations for deploying blockchain do so because they have enough storage and processing power.

Lightweight blockchain-based registration and authentication mechanism: The fact that the nodes are deployed in a hostile and unmanaged environment necessitates node authentication.

Optimized deep learning based malicious node identification: The performance of the network is impacted by the existence of malicious nodes after the network has been deployed. The suggested technique employs a Deep Belief Network-based CMPRO to identify attacker nodes in the network. To enhance the detection accuracy of the model, the hidden layers of DBN is optimized using the new hybrid optimization model (CMPRO).

Optimal path identification: When malicious nodes are found, the source node chooses the quickest route to the destination and uses secure routing when there are no harmful nodes. In the suggested concept, the Dijkstra algorithm is used to determine the optimal routes for data routing. Fig. 1 shows the architecture of the proposed work.

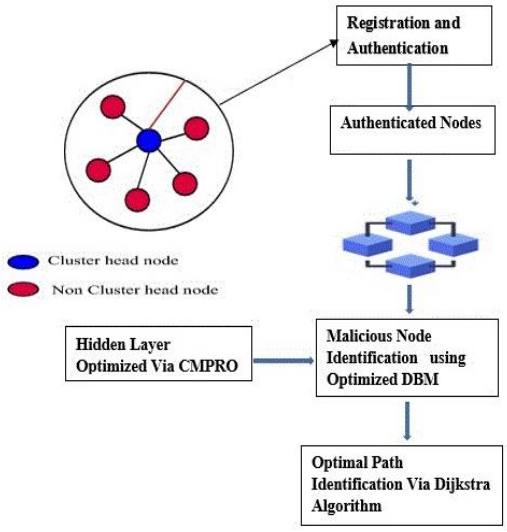

Figure 1. Architecture of the proposed work.

A. Network Deployment

The network is initially created using N (count = 100) nodes. One of those nodes will serve as the base station. Then, a certain number of nodes is chosen as the cluster head out of the remaining nodes (99 nodes). The CH's main duty is to compile sensed data from member nodes, put it together, and send it to the base station/sink. Based on the hybrid-two-fold objectives (like energy consumption and delay) and CMPRO, the optimal cluster head is chosen. Moreover, when two or more nearby nodes satisfy the two-fold objectives (energy consumption and delay), then the optimal node among them is selected using the CMPRO. The propose hybrid optimization model is the conceptual amalgamation of the standard ChOA and PRO method, respectively.

Energy consumption: The nodes are deployed randomly. The majority of the energy is lost during communication. For transmitting a -bit data from the transmitter to the receiver in a free-space multi-path fading channel, the transmitted energy T^{tx} is shown mathematically in Eq. (1). In addition, T^{ct} is the receiver energy consumed for transmitting 1-bit of data, T^{amp} is the data energy consumption of a 1-bit in multi-path attention mode and $\in$ is the data energy consumption of 1-bit in free space mode. The notation H_0 denotes the threshold distance, and it is computed as per Eq. (2).

$$T^{tx}(a,H) = \begin{cases} a \cdot T^{ct} + a \cdot \in \cdot H^2 & when\ H \le H_0 \\ a \cdot T^{ct} + a \cdot T^{amp} \cdot H^2 & when\ H > H_0 \end{cases} \quad (1)$$

$$H_0 = \sqrt{\frac{\in}{T^{amp}}} \quad (2)$$

In addition, the receiver energy consumption T^{Rx} is mathematically shown in Eq. (3).

$$T^{Rx} = a \cdot T^{ct} \quad (3)$$

Delay: The number of individuals who make up a cluster directly impacts the fitness function of delay. In order to decrease the latency, the clusters leader owns fewer members. The representation of the delay's fitness function is given by Eq. (4).

$$\sigma = \frac{\max(\|B_i - F_j\|) \cdot S_f}{S_f} \quad (4)$$

Here, S_f is the count of cluster nodes.

Moreover, block-chain is deployed on the CHs and base station because they have sufficient storage and computational resources.

B. Registration and Authentication

The fact that the nodes are deployed in a hostile and unattended environment necessitates node authentication. Nodes are more likely to be attacked by the attackers in this environment. These attackers gain physical access to targeted nodes and abuse their connections to the network. Additionally, hackers can use the nodes' IDs to re-enter the network and carry out other nefarious deeds. As a result, various blockchain-based mechanisms for registration and authentication have been proposed, where the likelihood of malicious node behaviour is greatly reduced. Although

hashes are stored on the blockchain and can be guessed by various methods, such as a brute force attack, there are still opportunities for various types of attacks that can be carried out by manipulating the network nodes' login credentials. In light of this, a safe and portable registration and authentication mechanism is suggested. However, compared to conventional storage methods, blockchain storage is very expensive. To reduce the weight of storage required by blockchain, the registration and authentication processes are made simple. The system will benefit less from our network's requirements because nodes have a finite amount of time for communication. As a result, the attackers won't be able to access the nodes or guess the hashed value of the credentials until their lifetime is over. The registration and authentication mechanism's detailed and step-by-step workflow is listed below:

Step 1: Sending the credentials to blockchain C is the first step in the registration process. The package of registration request req⟶C contains identity of the sensor node ID_S and location of the node P_S.

$$Reg_{Req\rightarrow C} = (ID_S, P_S) \quad (5)$$

Step 2: Using blockchain, a distinct three-digit number No. 'unique' is generated. To prevent hashes from colliding, these digits is added to the aforementioned package. The node will receive the special number as its password for all upcoming communications.

$$C \longrightarrow hashing + \left(ID_S, P_S, No_{unique}\right)_{hash} \quad (6)$$

Step 3. The blockchain stores the hash and the unique number for use in the future, such as authentication. Even if the attacker learned the node's ID and location, the hashes is transformed into cypher text, rendering them indecipherable.

Step 4. If a node wants to access the network after successfully registering, it will send an authentication request to the blockchain. The authentication request's package includes the information below.

$$Auth_{req\rightarrow C} = \left(ID_S, P_S, No_{unique}\right) \quad (7)$$

Step 5. The credentials listed above is hashed by the blockchain, which will then compare it to hashes that have already been stored. The sensor nodes are able to successfully communicate if the match is successful, thanks to blockchain. If not, an authentication error message will appear.

Step 6. Following the authentication procedure, the source node transmits the data packets to the destination node via intermediary nodes like Optimal CHs, which carry out secure routing by storing the routing information on the blockchain.

C. Malicious Node Identification

The presence of MNs in the network after network deployment affects network performance. The performance of the network is impacted after network deployment by the presence of malicious nodes. The new hybrid optimization model (ChoA+PRO) based Deep Belief Network is used in the proposed model to identify malicious nodes.

Deep Belief Network: A Deep Belief Network (DBN) is a sophisticated generative model that employs a deep architecture. There have also been presented RBM and DBM as additional pre-training techniques. RBMs could function as the DNN's nuclear component. In a nutshell, a Boltzmann Machine is a stochastic neural network in which every neuron is connected to every other neuron in both directions and there are no discrete "layers". This structure is transformed into a more conventional one by an RBM. There are dedicated input and output layers with only unidirectional connections connecting neurons in different layers. Fig. 2 shows a model for such a system. The network can be trained much more quickly thanks to the distinct relationship between the input and output layers. The RBM also has the benefit of being easily expandable by allowing the input layer of one RBM to function as the output layer of another RBM.

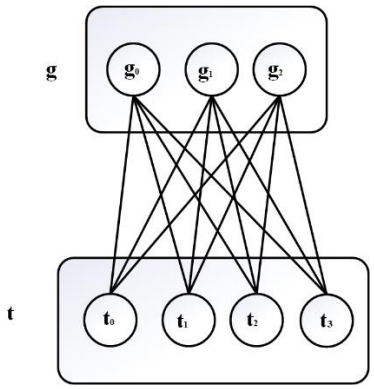

Figure 2. RBM: A graphical model that is not directed and has two layers: One with hidden units (g) and one with visible units (t).

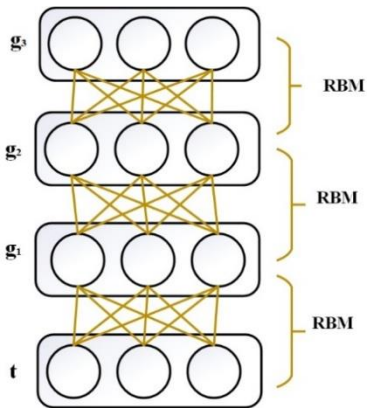

Figure 3. DBN with hidden layers in addition to one visible layer.

This method of cascading multiple RBMs results in a neural network with multiple hidden layers, also known as a DBN, as shown in Fig. 3. Although on the surface, this looks like a multi-layer feedforward neural network, the way the network is trained is different. Each RBM is specifically added to the network one layer at a time and trained unsupervised before backpropagation and supervised learning are applied to the entire network. With this approach, a DBN can independently choose the important features to analyses and is not subject to the unreasonably long convergence times of networks that only

use back-propagation to change the weights among their numerous layers. The contrastive divergence algorithm, which is outlined below, is the unsupervised learning technique frequently used in this context.

A RBM has the general form of an energy function for a pair of visible and hidden vectors $< t;\ g >$ with a matrix of weights V related to the connection between t and g as follows:

$$T(t,g) = -b^Y t - d^Y g - t^Y V g \tag{8}$$

where b and d are the bias weights for visible units and hidden units respectively. Probability distributions of t and g are constructed in terms of T:

$$Q(t,g) = \frac{1}{F} f^{-T(t,g)} \tag{9}$$

where F is a normalising variable, whose definition is given in Eq. (10).

$$F = \sum_{t'g'} f^{-T(t'g')} \tag{10}$$

The probability of a vector t also equals the product of the aforementioned equation over all hidden units:

$$Q(t) = \frac{1}{F} \sum_g f^{-T(t,g)} \tag{11}$$

The following formula is used to compute the log-likelihood of training data with respect to V:

$$\sum_{m=1}^{m=M} \frac{\partial log Q(t^m)}{\partial V_{ik}} = \langle t_i g_i \rangle_{inf} - \langle t_i g_i \rangle_{mdl} \tag{12}$$

where$\langle \cdot \rangle_{inf}$ and $\langle \cdot \rangle_{mdl}$ indicate expected values in the data or model distribution. The following are the learning guidelines for network weights in the log-likelihood-based training data:

$$\Delta V_{ik} = \varepsilon \left(\langle t_i g_i \rangle_{inf} - \langle t_i g_i \rangle_{mdl} \right) \tag{13}$$

where ε is the rate of learning. Since there is no connection between the neurons at either the hidden or visible layer, unbiased samples can be achieved from $\langle t_i g_i \rangle_{inf}$. Additionally, depending on whether hidden or visible units are present, the activations of those units are conditionally independent. Consider the following definition of the conditional property of g given t:

$$Q(g|t) = \prod_k Q(g_k|t) \tag{14}$$

where, $g_k \in \{0,1\}$ and the probability of $g_k = 1$ is:

$$Q(g_k = 1|t) = \sigma(d_k + \sum_i t_i V_{ik}) \tag{15}$$

where, σ is logistic function defined as:

$$\sigma(z) = (1 + f^{-z})^{-1} \tag{16}$$

The conditional probability of t_i =1 is calculated similarly, as follows:

$$Q(t_i = 1|t) = \sigma(b_i + \sum_k V_{ik} g_k) \tag{17}$$

The application of unbiased sampling from $\langle t_i g_i \rangle$ is not simple in general, but it can be achieved by sampling a reconstruction of the visible units from hidden units first, followed by multiple iterations of Gibbs sampling. Eq. (15) is used to update all hidden units simultaneously using Gibbs sampling, and Eq. (17) is then used to update all visible units. Finally, by computing the expected value of multiplying the updated values for hidden and visible units, the proper sampling from $\langle t_i g_i \rangle$ could be accomplished. The RBM weights can be used to initialise feedforward neural networks with sigmoid hidden units using sigmoid Eqs. (15) and (17) respectively. To enhance the detection accuracy of the model, the hidden layers of DBN is optimized using the new hybrid optimization model (CMPRO).

CMPRO: The proposed CMPRO model is the conceptual amalgamation of ChoA and PRO. Chimp Optimization Algorithm (ChOA) inspired by the individual intelligence and sexual motivation of chimps in their group hunting, which is different from the other social predators. The input to CMPRO model is the hidden neurons of DBN. ChOA is designed to further alleviate the two problems of slow convergence speed and trapping in local optima in solving high-dimensional problems. The Poor and Rich Optimization (PRO) is inspired by the efforts of the two groups of the poor and the rich to achieve wealth and improve their economic situation. The rich always try to increase their class gap with the poor by gaining wealth from different ways. The design of PRO is based on a genuine social phenomenon that can be used as a solution to challenging optimization issues. In the CMPRO model, the ChoA model is deployed within PRO model. The five steps of the CMPRO algorithm are described in this section.

Initial population: The CMPRO algorithm generates a uniform distribution of upper bound and lower bound parameters among a randomly chosen initial population based on PRO. The output of the objective function is then used to evaluate and sort this initial population in ascending order. Two subpopulations make up the main population in the CMPRO algorithm. The first subpopulation is associated with the wealthy, whereas the second is associated with the underprivileged. Depending on the issue, these two subpopulations can range in size. The CMPRO algorithm's primary population is depicted in Eq. (18):

$$PP_{Nim} = PP_{Npr} + PP_{Nrc} \tag{18}$$

where PP_{Nim}, PP_{Npr} and PP_{Nrc} demonstrate the size of main inhabitants, poor population and rich population, respectively. The rich population is related to the first part of the main population, which is sorted in ascending order, and the poor population is related to the second part. In actuality, the CMPRO algorithm gives better positions to all members of the wealthy population than to those of the poor population. In CMPRO, Eq. (19) is always true:

$$prc_1 < prc_2 < prc_3 < \cdots < prc_m < prc_{m+1} < prc_{m+2} < prc_{m+3} < \cdots < prc_n \tag{19}$$

Updating the positions: The subpopulations of the rich and the poor make up the main population in the CMPRO algorithm. Every time the algorithm iterates, a predetermined mechanism must be used to adjust each population member's position.

The change in the position of each rich population member: In any iteration of the CMPRO algorithm, the position of each member of the wealthy population shifts in accordance with Eq. (20):

$$\overrightarrow{Y_{rc,a}^{fr}} = \overrightarrow{Y_{rc,a}^{od}} + t\left[\overrightarrow{Y_{rc,a}^{od}} - \overrightarrow{Y_{pr,best}^{od}}\right] \quad (20)$$

where $\overrightarrow{Y_{rc,a}^{fr}}$ is the different standards of the ath position of the rich population, $\overrightarrow{Y_{rc,a}^{od}}$ is the face amount of the ath position of the rich population, t is the class gap parameter $\overrightarrow{Y_{pr,best}^{od}}$ is the present position of the best member of the poor population. The value of Y is accounted as a vector of all variables. In fact, all members of the rich population increase its distance from every member of the poor population by getting richer. Since $\overrightarrow{Y_{pr,best}^{od}}$ is the best member of the poor population, when a member of the rich population increases the distance from $\overrightarrow{Y_{pr,best}^{od}}$ its span from all members of the poor population is increased. In fact, the distance between the poor and the rich gets higher when the people in poverty gets poorer.

Each member of the rich population should maintain a certain distance from the poor population, which is determined randomly by the random number between 0 and 1 known as t. The rich population experiences internal competition as a result of t's randomness. In other words, t determines each member's improvement when two members of the rich population are close to one another and $\overrightarrow{Y_{pr,best}^{od}}$ is fixed. It implies that positions with higher costs may experience more improvements when using higher t values than positions with lower costs.

The change in the position of each poor population member via Driving and chasing the prey phase of ChoA model (proposed): In each iteration of the CMPRO algorithm, the position of each member of the poor population shifts in accordance with Eq. (21). In this phase, the Driving and chasing the prey phase of ChoA is used to update the position of the search agent. As per the proposed model, the coefficient vectors m, C, d are newly added to enhance the convergence speed of the solutions.

$$\overrightarrow{Y_{pr,a}^{fr}} = \left|\overrightarrow{C \cdot Y_{pr,a}^{od}} + \left[t(patt) - m \cdot \overrightarrow{Y_{pr,a}^{od}}\right] \cdot d\right| \quad (21)$$

$$C = 2 \cdot rand2 \quad (22)$$

$$m = chaotic\_value \quad (23)$$

where $\overrightarrow{Y_{pr,a}^{fr}}$ is the new value of the ath position of the poor population, $\overrightarrow{Y_{pr,a}^{od}}$ is the present value of the ath position of the poor population, t is the pattern improvement parameter (with a random value between 0 and 1) and the pattern of getting rich. Eq. (24) gives the pattern value:

$$patt = \frac{\overrightarrow{Y_{rc,best}^{od}} + \overrightarrow{Y_{rc,mn}^{od}} + \overrightarrow{Y_{rc,wst}^{od}}}{3} \quad (24)$$

where $\overrightarrow{Y_{rc,best}^{od}}$ is the best member of positions in the rich population, $\overrightarrow{Y_{rc,mn}^{od}}$ is the average position of the rich population members while $\overrightarrow{Y_{rc,wst}^{od}}$ is the position of the worst member in the rich population. The average position of three wealthy representatives is sought after in each iteration because attaining wealth differs for each individual. The random parameter t determines the pattern improvement and, as a result, the improvement in $\overrightarrow{Y_{pr,a}^{od}}$ because the pattern value is fixed in each iteration. In fact, when the t value is close to 0, more improvement is seen in the pattern; and since $\overrightarrow{Y_{pr,a}^{od}}$ is greater than the pattern value, it will have a greater improvement and vice versa. Arbitrariness of t causes an internal competition in the poor population. It means that the little value of t leads to more improvement in the pattern, and where the positions are close to each other, the t value causes changes in rank of these positions.

Social incentive-based mutation (proposed): In this phase, the social motivation is newly introduced within the mutation phase of PRO model. This newly added chaotic behavior in mutation phase helps search agents to further alleviate the two problems of entrapment in local optima and slow convergence rate in solving high-dimensional problems. The Social incentive-based mutation for the rich and poor populations is determined by Eqs. (23) and (24), respectively. A random number μ is generated between [0,1].

If $\mu < P_{mut}$ (Mutation probability), the new value of the rich population is updated using the new expression given in Eq. (25).

$$\overrightarrow{Y_{rc,a}^{fr}} = \overrightarrow{Y_{rc,a}^{fr}} - a \cdot \overrightarrow{Y_{pr,a}^{fr}} \quad (25)$$

Here, a is the coefficient vector that is computed as per Eq. (26). Moreover, f is reduced linearly from 2.5 to 0.

$$a = 2 \cdot f \cdot rand1 - f$$

$$if\ \mu < P_{mut}$$

$$\overrightarrow{Y_{pr,a}^{fr}} = \overrightarrow{Y_{pr,a}^{fr}} + rand1 \quad (26)$$

End

As a consequence, the malicious node in the network is identified using blockchain.

D. Shortest Path for Routing

In the third step, which follows the detection of MNs, the source node chooses the quickest route to the destination and executes secure routing in the absence of Malicious Node (MN). The Dijkstra algorithm is employed in the suggested model to determine the shortest path, and it takes into account every route that leads from the source to the destination node. After determining the shortest path based on the weights assigned to each node's edge, the nodes' energy consumption is reduced.

IV. Result and Discussion

A. Experimental Setup

The proposed model has been implemented in PYTHON. The data for evaluation has been collected from dataset 1 (https://www.kaggle.com/datasets/pedrohauy/sampledtftp attackcicddos2019) and database 2 (https://www.kaggle.com/datasets/solarmainframe/ids-

intrusion-csv). Among the collected data, 70% of the data has been for training purpose, and the rest 30% of the data has been used for testing purpose. This section elaborates the graphical analysis for optimized deep learning based malicious nodes detection in intelligent sensor-based systems using blockchain. The graphs are compared with various existing techniques like Manta Rays Foraging Optimization Algorithm (MRFO), Black Widow Optimization (BWO) and Random Forest (RF). The performance metrics like Accuracy, FNR, FPR, MCC, NPV, precision, sensitivity, specificity and F-measure are used to evaluate the proposed model.

B. Performance Analysis of the Proposed Model

1) Analysis of accuracy

Analysis of accuracy using various existing technique is shown in Fig. 4. In proposed, when the value of learn rate is 60%, 70% and 80% then the value of accuracy is 0.9, 0.901 and 0.902. The outcome of the proposed technique is high compared to existing technique. This improvement is owing towards the selection of the optimal CH.

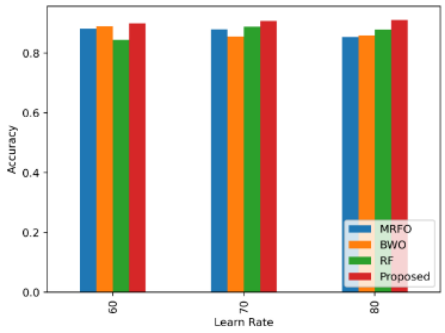

Figure 4. Analysis on the performance of the proposed work in terms of accuracy.

2) Analysis of F-Measure

Analysis of F-Measure using various existing technique is shown in Fig. 5. In proposed, when the value of learn rate is 60%, 70% and 80% then the value of F-Measure is 0.86, 0.81 and 0.9. Compared to existing technique the proposed technique high in F-Measure.

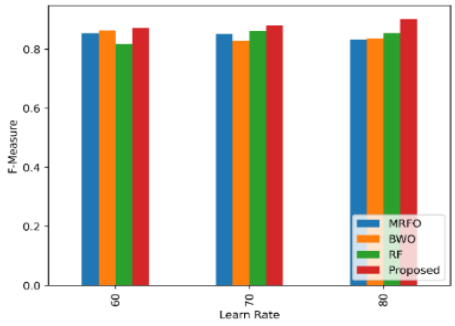

Figure 5. Analysis on the performance of the proposed work in terms of F-Measure.

3) Analysis of False Negative Rate (FNR)

Analysis of FNR using various existing technique is shown in Fig. 6, when the value of learn rate is 60%, 70% and 80% then the value of accuracy is 0.16, 0.22 and 0.06. Compared to existing technique the proposed technique is low. The reduction in error performance is due to the optimization of hidden layers of DBN with the new hybrid optimization model.

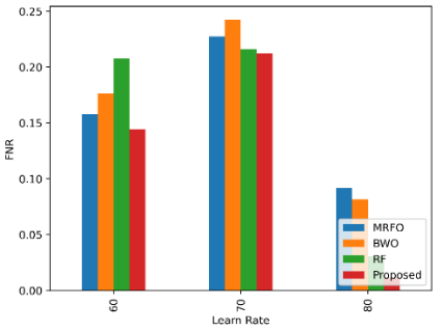

Figure 6. Analysis on the performance of the proposed work in terms of FNR.

4) Analysis of False Positive Rate (FPR)

Analysis of FPR using various existing technique is shown in Fig. 7, when the value of learn rate is 60%, 70% and 80% then the value of FPR is 0.17, 0.16 and 0.04. Compared to existing technique the proposed technique is low.

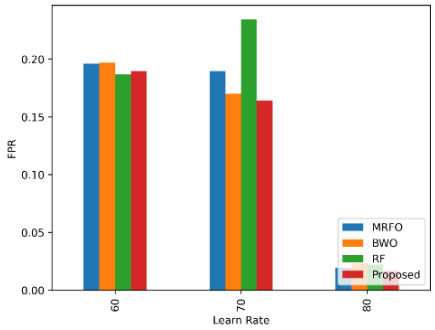

Figure 7. Analysis on the performance of the proposed work in terms of FPR.

5) Analysis of Matthew's Correlation Coefficient (MCC)

Analysis of MCC using various existing technique shown in Fig. 8, when the value of learn rate is 60%, 70% and 80% then the value of MCC is 0.203, 0.204 and 0.9.

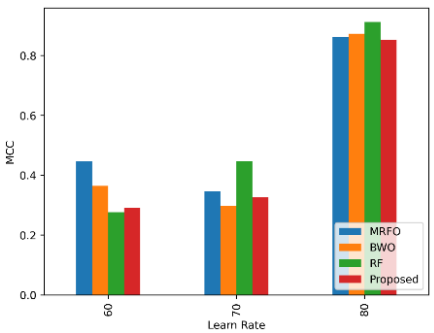

Figure 8. Analysis on the performance of the proposed work in terms of MCC.

6) Analysis on Negative Predictive Value (NPV)

Analysis of NPV using various existing technique is shown in Fig. 9, when the value of learn rate is 60%, 70%

and 80% then the value of FPR is 0.9, 0.91 and 0.84. Compared to existing method the NPV feature of proposed method in high.

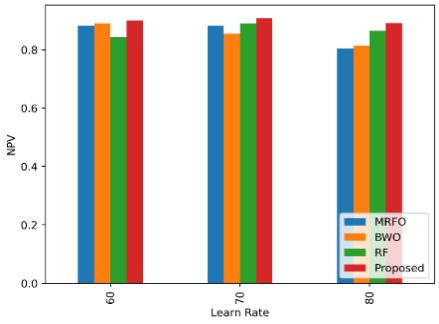

Figure 9. Analysis on the performance of the proposed work in terms of NPV.

7) Analysis of precision

Examination of precision using various existing technique is shown in Fig. 10, when the value of learn rate is 60%, 70% and 80% then the value of precision is 0.91, 0.92 and 0.83. Compared to existing method the precision feature of proposed method in high.

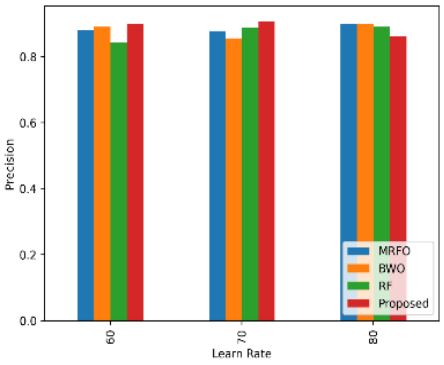

Figure 10. Analysis on the performance of the proposed work in terms of Precision.

8) Analysis of sensitivity

Fig. 11 displays the investigation of sensitivity using various existing technique, when the value of learn rate is 60%, 70% and 80% then the value of precision is 0.89, 0.91 and 0.9. The sensitivity of proposed technique is high compared to existing technique.

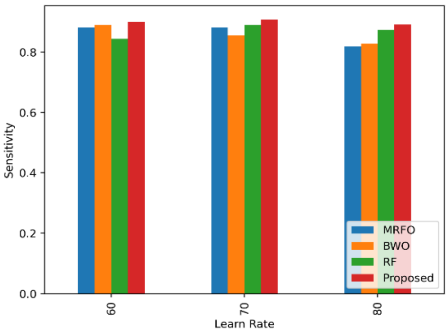

Figure 11. Analysis on the performance of the proposed work in terms of Sensitivity.

9) Analysis of specificity

Analysis of specificity using various existing technique is shown in Fig. 12, when the value of learn rate is 60%, 70% and 80% then the value of precision is 0.91, 0.92 and 0.7. The specificity of proposed technique is high compared to existing technique. Thus, the proposed model is said to be significant for malicious node identification in blockchain model.

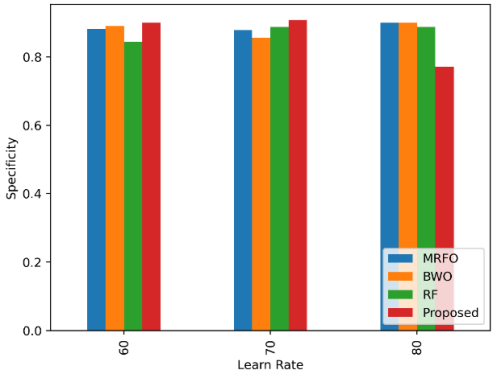

Figure 12. Analysis on the performance of the proposed work in terms of Specificity.

V. Conclusion

This research work has introduced a new blockchain-based secure routing model for Internet of Sensor Things (IoST) for secured data routing. For the Internet of Sensor Things (IoST), this research work has introduced a new blockchain-based secure routing model for data routing. At first, the system has been tested, and the best cluster head was chosen using the new Chimp Social Incentive-based Mutated Poor Rich Optimization Algorithm, which has two objectives (energy consumption and delay) (CMPRO). The standard Chimp Optimization Algorithm (ChOA) and the Poor and Rich Optimization (PRO) method are conceptually combined in the proposed CMPRO. Additionally, the ideal CHs and base stations for deploying blockchain do so because they have enough storage and processing power. A simple blockchain-based registration and authentication mechanism was further implemented. The new Optimized Deep Belief Network has been used to identify malicious nodes in the network following network authentication. The hidden layers of the DBN model have been optimised using the new hybrid optimization model to increase the model's detection accuracy (CMPRO). When malicious nodes are found, the source node chooses the quickest route to the destination and uses secure routing whenever there are no malicious nodes. In the suggested model, the Dijkstra algorithm is used to determine the best route for data routing. The network is secured as a whole. Finally, the model's performance is verified to demonstrate its superior efficiency to other models. Analysis of accuracy using various existing technique is shown in Fig. 3, when the value of learn rate is 60%, 70% and 80% then the value of accuracy is 0.9, 0.901 and 0.902. The outcome of the proposed technique is high compared to existing technique.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

Swathi Darla and Naveena C have participated in the design of the proposed method. Swathi Darla has implemented, coded the method and done testing and obtained the results. As a supervisor, Naveena C supporting and guiding Swathi Darla during her research work with some ideas and knowledge. Both authors read and approved the final manuscript.

REFERENCES

[1] T. Qiu, K. Zheng, M. Han, C. P. Chen, and M. Xu, "A data-emergency-aware scheduling scheme for Internet of Things in smart cities," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 2042–2051, 2017.

[2] A. Abdollahi, K. Rejeb, A. Rejeb, M. M. Mostafa, and S. Zailani, "Wireless sensor networks in agriculture: Insights from bibliometric analysis," *Sustainability*, vol. 13, no. 21, 12011, 2021.

[3] E. Niewiadomska-Szynkiewicz, A. Sikora, J. Kołodziej, and P. Szynkiewicz, "Modelling and simulation of secure energy aware fog sensing systems," *Simulation Modelling Practice and Theory*, vol. 101, 102011, 2020.

[4] A. F. Khan and G. Anandharaj, "AHKM: An improved class of hash based key management mechanism with combined solution for single hop and multi hop nodes in IoT," *Egyptian Informatics Journal*, vol. 22, no. 2, pp. 119–124, 2021.

[5] A. Ahad, M. Tahir, and K. L. A. Yau, "5G-based smart healthcare network: Architecture, taxonomy, challenges and future research directions," *IEEE Access*, vol. 7, pp. 100747–100762, 2019.

[6] R. Kashyap, "Applications of wireless sensor networks in healthcare," in *IoT and WSN Applications for Modern Agricultural Advancements: Emerging Research and Opportunities*, IGI Global, 2020, pp. 8–40.

[7] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and M. Imran, "Perception layer security in Internet of Things," *Future Generation Computer Systems*, vol. 100, pp. 144–164, 2019.

[8] J. P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations," *International Journal of Information Security*, vol. 21, no. 1, pp. 115–158, 2022.

[9] A. Shankar, P. Pandiaraja, K. Sumathi, T. Stephan, and P. Sharma, "Privacy preserving e-voting cloud system based on ID based encryption," *Peer-to-Peer Networking and Applications*, vol. 14, no. 4, pp. 2399–2409, 2021.

[10] S. Abbas, N. Javaid, A. Almogren, S. M. Gulfam, A. Ahmed, and A. Radwan, "Securing genetic algorithm enabled SDN routing for blockchain based Internet of Things," *IEEE Access*, vol. 9, pp. 139739–139754, 2021.

[11] A. S. Yahaya, N. Javaid, A. Almogren, A. Ahmed, S. M. Gulfam, and A. Radwan, "A two-stage privacy preservation and secure peer-to-peer energy trading model using blockchain and cloud-based aggregator," *IEEE Access*, vol. 9, pp. 143121–143137, 2021.

[12] W. She, Q. Liu, Z. Tian, J. S. Chen, B. Wang, and W. Liu, "Blockchain trust model for malicious node detection in wireless sensor networks," *IEEE Access*, vol. 7, pp. 38947–38956, 2019.

[13] D. Sivaganesan, "A data driven trust mechanism based on blockchain in IoT sensor networks for detection and mitigation of attacks," *Journal of Trends in Computer Science and Smart Technology (TCSST)*, vol. 3, no. 1, pp. 59–69, 2021.

[14] M. B. E. Sajid, S. Ullah, N. Javaid, I. Ullah, A. M. Qamar, and F. Zaman. Exploiting machine learning to detect malicious nodes in blockchain enabled Internet of Sensor Things. [Online]. Available: https://www.researchgate.net/profile/Ibrar-Ullah-3/publication/356988153_Exploiting_Machine_Learning_to_Detect_Malicious_Nodes_in_Intelligent_Sensor-Based_Systems_Using_Blockchain/links/61d70209da5d105e5522a6c7/Exploiting-Machine-Learning-to-Detect-Malicious-Nodes-in-Intelligent-Sensor-Based-Systems-Using-Blockchain.pdf

[15] N. Tariq, M. Asim, F. A. Khan, T. Baker, U. Khalid, and A. Derhab, "A blockchain-based multi-mobile code-driven trust mechanism for detecting internal attacks in internet of things," *Sensors*, vol. 21, no. 1, p. 23, 2020.

[16] X. Wu and J. Liang, "A blockchain-based trust management method for Internet of Things," *Pervasive and Mobile Computing*, vol. 1, no. 72, 101330, 2021.

[17] G. Ramezan and C. Leung, "Wireless communications and mobile computing," *Wireless Communications and Mobile Computing*, 4029591, 2018.

[18] S. Hong, "P2P networking based Internet of Things (IoT) sensor node authentication by blockchain," *Peer-to-Peer Networking and Applications*, vol. 13, no. 2, pp. 579–589, 2020.

[19] K. Haseeb, N. Islam, A. Almogren, and I. U. Din, "Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things," *IEEE Access*, vol. 7, pp. 185496–185505, 2019.

[20] M. H. Kumar, V. Mohanraj, Y. Suresh, J. Senthilkumar, and G. Nagalalli, "Trust aware localized routing and class based dynamic block chain encryption scheme for improved security in WSN," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 5, pp. 5287–5295, 2021.

[21] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, and Y. Zhang, "A blockchain-based nonrepudiation network computing service scheme for industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3632–3641, 2019.