iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** I **Month of publication:** January 2026

DOI: https://doi.org/10.22214/ijraset.2026.77080

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue I Jan 2026- Available at www.ijraset.com

Linear Regressive Momentum Optimized Dense Neural Network for Energy and Secure Data Transmission in WSN

D. Mohanapriya[1], Dr. V. Saravanan[2]
[1]*Research Scholar & Assistant Professor, Department of Information Technology, Hindusthan College of Arts & Science College, Coimbatore, Tamilnadu, India*
[2]*Professor & HEAD, Department of Information Technology, Hindusthan College of Arts & Science College, Coimbatore, Tamilnadu, India*

Abstract: ***Wireless Sensor Networks (WSNs) is a distributed network initially designed as simple monitoring systems comprising numerous sensor nodes focusing on data collection, processing, and transmission. In WSNs, a huge amount of vulnerabilities can arise, specifically those initiating from malicious nodes (MNs), which direct to cooperate data integrity, network stability, and reliability. Although security remains critical, current MN detection methods are time-consuming and increased latency for constrained WSNs. In order to overcome these issues, a novel Linear Regressive Momentum Optimized Dense neural Network (LiRMO-DenseNet) model is developed to enhance the data transmission security in WSN. The proposed LiRMO-DenseNet model utilizes the dense neural network concept to categorize the sensor nodes as legitimate sensor nodes or intruders with help of several layers such as input, numerous hidden layers, and output layer. First, the number of sensor nodes is given to the input layer. After that, the input layer transmits the collected sensor nodes to the first hidden layer. In that layer, the different characteristics of the sensor nodes like energy, cooperativeness and trust level are computed. Then, the computed values of the sensor nodes are given to third hidden layer. In that layer, Changepoint linear regression analysis is carried out for analyzing the sensor node with their characteristics by setting the threshold. Depending on the analysis, the nodes are classified as legitimate sensor nodes and intruders. A new part of this process is fine-tuning of dense neural network, where the Metaheuristic Walrus Optimization algorithm is employed to update the hyperparameter of dense neural network for minimizing the training and validation errors, thereby boosting the accuracy of node classification. Finally, the accurate node classification is carried out at output layer. With the selected legitimate sensor nodes, secure data transmission is achieved in WSN. The effectiveness of the proposed LiRMO-DenseNet model is assessed using a comprehensive set of performance measures, including accuracy, confidentiality rate, data integrity rate, packet delivery rate, throughput and delay. The simulation findings demonstrate that the proposed LiRMO-DenseNet model consistently achieves superior security performance, exhibiting higher confidentiality and reduced delay compared to existing deep learning based methods.***

Keywords: ***WSN, secure data transmission, dense neural network, Changepoint linear regression analysis based legitimate node classification, Metaheuristic Walrus Optimization algorithm based fine tuning.***

I. INTRODUCTION

Wireless sensor networks (WSNs) have gain significant attention due to their low-power intelligent processing, compact node size, self-organizing capabilities, and efficient routing. These networks support a wide range of applications, including home automation, smart city infrastructure, health monitoring, and object tracking. Sensor nodes are typically small and battery-powered, which entails inherent limitations related to energy availability, and overall computational resources. Owing to their communication patterns and deployment environments, WSNs face critical challenges in energy management and secure data transmission, both of which directly impact network lifetime and resilience against malicious nodes. To address energy constraints and security of data transmission, various techniques have emerged as effective solutions for prolonging the operational lifetime of the network.

Quantum search-enhanced bat algorithm (QS-BAT) was designed in [1] for accurate intrusion detection based on deep learning architectures under multiple attack scenarios. However, accuracy, latency, and energy consumption remained major challenges in distributed IDS deployments. Machine Learning-based Secure Routing Protocol (MLSRP) was developed in [2] for WSN to obtain better energy efficiency and deliver an efficient security with reduced data loss. However, deep learning model was not employed for achieving higher accuracy in intruder node detection.

©IJRASET: All Rights are Reserved

An efficient Multi-Level Trust Based Secure Routing (MLTSR-BC) was presented in [3] for secure transmission of data between the nodes within the network. The designed mode increases the data security and throughput. However, intruder nodes within the network were not accurately identified. An Improved Type-2 Fuzzy Logic System (IT2FLS) was developed in [4] for secure and energy-efficient routing with minimal delay and higher throughput by means of the Reptile Search Algorithm. However the network complexity and security threats were major concern for reliable communication in complex technological environments. In order to enhance the reliable data transmission, modular Artificial Intelligence (AI)-based routing framework was introduced in [5] for WSN. However, the accuracy of the framework remained unaddressed. Secure Machine-learning-based Adaptive Reliable Trust (SMART) model was introduced in [6] for enhanced security and accuracy based on trust values. However, fine-tuning the model did not perform to verify and enhance its robustness and reliability. An energy-aware and adaptive intrusion detection system was developed in [7] for WSNs to detect the Black Hole and Wormhole attacks on the routing systems. However, the energy-sensitive routing functions did not integrated to minimize the computational load. Secure cluster-based routing model was designed in [8] based on residual energy, trust, node degree, and location factors. However, it did not integrate advanced optimization techniques to minimize energy consumption while considering a large number of nodes. AI-driven authentication system was introduced in [9] to increase the security and reliability of sensor nodes. Though the model achieves high detection rates, accurate trust scores, minimal latency, and competitive energy consumption, higher throughput was not achieved. A Deep Learning-Enhanced Hybrid Trust (DLEHT) model was developed in [10] to greatly increase the security and performance of WSNs with higher packet delivery and packet drop reduction. However, the accuracy of intruder node detection was a major issue. Effective machine learning (ML) technique was developed in [11] to enhance the routing security. However, deep learning (DL) model was not implemented to further enhance the security of data transmission. A fuzzy deep reinforcement learning (FDRL) was developed in [12] to enhance the energy efficient and secure data throughput. However, lightweight AI-driven heuristics algorithms were not designed to minimize the computational overhead. A new hybrid trust-based routing framework was introduced in [13] for secure, energy-efficient, and scalable communication. However, the framework was not applicable for heterogeneous and mobile IoT environments. Trusted Energy-Aware Hierarchical Routing (TEAHR) framework was developed in [14] for multi-level trust evaluation that enhances the security level. However, computational and energy overhead was not feasible for highly dynamic networks. Energy-Efficient Elliptic Diffie Clustering Technique (3EDCT) method was designed in [15] for energy balance security robustness. The designed technique reduces the communication and computation overhead. However, AI-driven trust evaluation and real-time anomaly detection was not performed to further strengthen the security.

A. Research contribution

The major contribution of the LiRMO-DenseNet model is summarized as given below,

1) A novel LiRMO-DenseNet model is developed to improve energy-efficient and secure data transmission in WSNs. This dense neural network-based approach integrates various processes, sensor node classification and secures data transmission.

2) To increase the classification accuracy, a dense neural network is employed to classify the sensor nodes based on their residual energy levels, cooperativeness and trust score. The changepoint linear regression is employed for analyzing the node and classified into legitimate and intruder nodes. The Walrus Optimization algorithm is employed to reduce the classification errors, thereby increasing the performance of precision, and recall.

3) To improve the secure data transfer rate and throughput, the LiRMO-DenseNet model utilizes the legitimate sensor nodes to transmit the data from sender to sink node.

4) Finally, an extensive simulation is conducted to analyze the performance of LiRMO-DenseNet model and other existing works.

B. Organization of the Paper

The remainder of this paper is structured into five sections. Section 2 reviews existing studies and outlines the background information. Section 3 details the proposed LiRMO-DenseNet model along with its architectural framework. Section 4 presents the simulation environment and discusses the obtained results. Section 5 provides a comparative analysis of different approaches based on multiple performance metrics. Finally, Section 6 concludes the paper by summarizing the key findings.

II. RELATED WORKS

A new Secure Clustering and Sleep-Wakeup based Energy Efficient Routing was introduced in [16] using Fennec fox optimized deep learning framework to minimize the energy usage and extend the network lifetime. However, designing lightweight deep learning strategies was major issue for resource-constrained nodes, and enhancing the security model to handle various attacks.

A deep gradient descent multi-layer Marquardt vector algorithm was designed in [17] for energy efficiency analysis and security analysis to achieve high throughput and minimize the delay. However, the model was not efficient in handling the dynamic nature of WSNs to improve the data transmission effectiveness. An intrusion detection framework based on deep learning was designed in [18] to increase the detection accuracy and minimize adversarial vulnerability. However, it failed to develop more reliable deep learning models for guaranteeing the security of WSNs. A lightweight machine learning (ML) approach was designed in [19] based on the extreme gradient boosting (XGBoost) model to distinguish various types of attacks with maximum accuracy. However secure data delivery performance was not achieved. Deep learning-based Intrusion Detection System (IDS) was developed in [20] to achieve both accurate and efficient threat detection. However, the latency aware threat detection remained major issue.

A novel improved bidirectional long-short-term memory (Bi-LSTM) algorithm was designed in [21] to address the issue of intrusion detection with higher accuracy. However, false positives and negatives were not addressed in intrusion detection. Lightweight MG-Net Model was introduced in [22] to addresses security by including a Trust Model, Anomaly Detection, and Secure Communication. However the model did not enhance the trust and cooperativeness for effectively improving the detection rate with minimum time. Adaptive Federated Reinforcement Learning-Hunger Games Search (AFRL-HGS) was developed in [23] for Secure and Reliable Data Transmission. However, the algorithm did not consider the other parameters such as trust, energy, and cooperativeness. A novel FireTG-Net model was introduced in [24] based on Firefly Swarm Optimization (FSO) for detecting anomalies within WSNs with higher detection accuracy. However it did not consider the energy aware trust modeling to optimize the network lifetime. Server–Client Machine Learning Intrusion Detection System (SC-MLIDS) was developed in [25] to enhance security by addressing the various threats. However more robust and responsive intrusion detection was major challenges.

An optimized ensemble method was introduced in [26] for the wireless networks against various attacks. However, the accuracy of various attack detection was not improved. In order to increase the accuracy, multi-deep learning intrusion detection framework was developed in [27]. However the model failed to focus on optimizing the model to enhance energy efficiency. Graph Neural Cryptonet (GNC-Net) was introduced in [28] for efficient trust-aware routing within the WSN environment. However, the model's scalability was not improved. Energy aware and secure routing (EASR) was developed in [29] for indentifying malicious behavior based on energy trust. However, machine learning and deep learning techniques failed to analyze comprehensive trust value for minimizing the computation overhead. A Dual Layer Security Framework (DLSF) was introduced in [30] to provide robust node authentication and secured communication using trust based approach. However, the framework did not support larger-scale deployments to further enhancing its robustness.

III. PROPOSAL METHODOLOGY

Wireless Sensor Networks (WSNs) comprises of small unit of sensor nodes equipped with processors, battery elements, and wireless communication units. These nodes gather information from the environment and transmit it to the sink node for further processing and decision-making. Due to the dynamic nature of networks, WSNs are devised to improve the processing capacity and data transmission effectiveness. However, secure data transmission remains a significant challenge in WSNs owing to increasing security risks. To address these concerns, the a novel LiRMO-DenseNet model is introduced to recognize resource-efficient and legitimate sensor nodes, thereby ensuring reliable and secure data communication across the network.

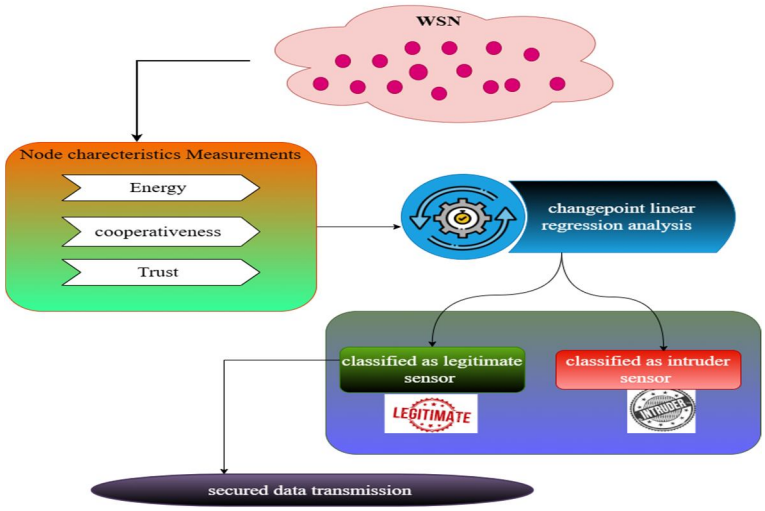


Figure 1: Architecture of the proposed LiRMO-DenseNet model

Figure 1 presents the architectural structure of the proposed LiRMO-DenseNet model developed for secure data communication in WSN. The proposed architecture utilizes the deep learning model for analyzing the key characteristics of the sensor nodes such as energy, cooperativeness and trust level. In the initial step, the measured characteristics of the sensor nodes are processed using a changepoint linear regression analysis method to precisely access node behavior. Based on the analysis outcome, each node is classified either as a legitimate sensor node or an intruder sensor node. Then the legitimate sensors are permitted to contribute the network operations, ensuring secure and reliable data transmission, while intruder sensors are detected and isolated to enhance the overall security and performance of the WSN. Each of these stages plays a vital role in the functioning of the proposed. Further details on these processes are described in the subsequent sections.

A. Network Model

The proposed model considers the network model specifically designed for secure data communication between the sensors to sink node. This model consists of a large number of low-power, energy-constrained sensor nodes $SN_i = SN_1, SN_2, SN_3 \dots SN_n$ in a $M \times M$ squared network area for sensing and collecting the data packets data packets $Dp_1, Dp_2, Dp_3, \dots Dp_n$ that has a similar sensible capacity and initial battery powers. In order to perform the secure communication, legitimate sensor nodes are identified based on three key characteristics such as energy (E), node cooperativeness (NC) and trust level (TL).

B. Dense Neural Network

The proposed LiRMO-DenseNet model utilizes the dense neural network (DNN), also called a Multi-Layer Perceptron (MLP) for identifying the legitimate or intruders sensor nodes. The dense neural network is a core artificial intelligence model where each neuron in one layer fully connected to neuron in the next succeeding layer, allowing it to learn complex patterns. Compared to traditional deep learning models, the proposed approach is capable of efficiently handling large volumes of input data. It processes information efficiently through parallel processing, allowing faster computation and improved performance. The structural layout of the proposed dense neural network model is illustrated in Figure 2.

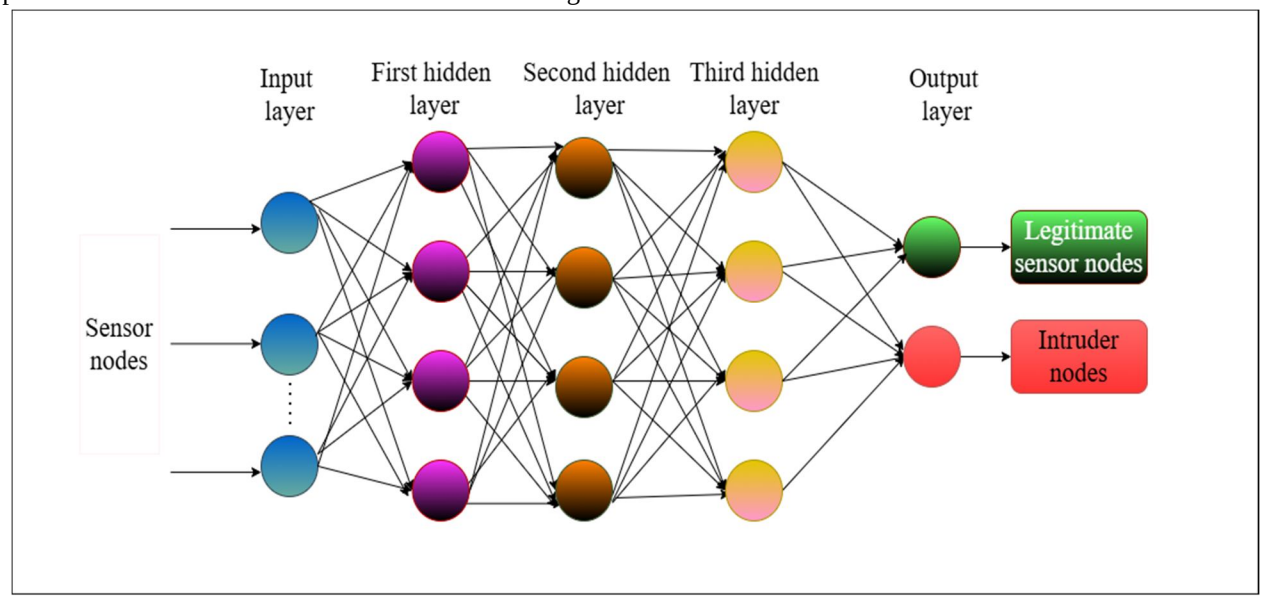


Figure 2 Structure of dense neural network

Figure 2 demonstrates the architecture of a dense neural network designed for secure data transmission in WSN. As depicted, the network consists of numerous layers, including input, hidden, and output layers. The input and output layers are single layers, whereas the hidden layers contain several sub-layers. Each layer consists of multiple units called artificial neurons or nodes. These neurons receive inputs, process them, and pass the results to neurons in the subsequent layer. The connections between neurons, referred to as synapses, are assigned weights that determine the strength of the links between layers.

Let us consider input i.e. sensor nodes $SN_1, SN_2, SN_3 \dots, SN_n$' given to the input layer of structure of the dense neural network architecture. The input sensor nodes are transferred to the one or more hidden layers positioned between the input and output layers. Each layer is made up of neurons that receive input from the previous layer.

For each neuron, the input is multiplied by specific weights that determine their importance, and then a bias term is added to shift the result. The neurons in the hidden layer computed the weighted sum as follows,

$$X = \sum_{i=1}^{n}(SN_i * Q_{ih}) + b \quad (1)$$

Where, X indicates an weighted sum output, Q_{ih} indicates a weights between input and hidden layer, number of sensor nodes 'SN_i', 'b represents a bias that stored the value is '1'.

At the beginning of the process, the entire sensor nodes are assumed to have equivalent initial energy. However, it performs sensing and monitoring operations, their energy levels decrease over time. Therefore, the total sensor energy consumption is estimated as follows,

$$EN_{con}^{SN_i} = EN_S + EN_{RX} + EN_{TX} \quad (2)$$

Where, $EN_{con}^{SN_i}$ indicates an energy consumption of i^{th} sensor node, EN_{TX} indicates an energy dispersed during transmission of a data, EN_P refers to an energy consumed during processing tasks, EN_S denotes an energy consumption of sensing the data.

$$EN_{TX}{}^{SN} = \left(EN_{el(TX)} * k_{TX}\right) + \left(EN_A * k_{TX} * D^2\right) \quad (3)$$

Where, $EN_{TX}{}^{SN}$ indicates a total energy consumed by the sensor node, k_{TX} denotes a size of the data being transmitted, $EN_{el(TX)}$ refers to energy dissipated by the transmitter electronics per bit, EN_A denotes a amplifier energy factor, D denotes a distance between the sensor nodes.

Energy consumed during the reception of data is calculated by multiplying the device's power consumption by the time taken to complete the processing tasks.

$$EN_{RX}{}^{SN} = EN_{el(RX)} * k_{RX} \quad (4)$$

Where, $EN_{RX}{}^{SN}$ indicates an energy dissipated during reception of a data, $EN_{el(RX)}$ refers to energy dissipated by the receiver electronics per bit, k_{RX} denotes a size of the data being received.

Therefore, the residual energy typically indicates the remaining energy in a sensor node after it executes the tasks such as sensing, communication, and processing.

$$EN_{res}\ (SN_i) = EN_{\ T}\ (SN_i) - EN_{con}^{SN_i} \quad (5)$$

Where, $EN_{res}\ (SN_i)$ represents the residual energy of i^{th} sensor node,$EN_{\ T}\ (SN_i)$ symbolizes total energy of i^{th} sensor node, $EN_{con}^{SN_i}$ indicates energy consumed by the i^{th} sensor node.

In this layer, the system evaluates cooperative each sensor node is in the network and assesses the trustworthiness of the nodes. This helps in identifying reliable nodes for data transmission and ensures that the network functions efficiently while minimizing malicious behavior.

The cooperativeness of the each sensor node is the ability of a node to actively participate in network activities, such as data forwarding, routing, and sharing resources. However, the attacker nodes do not cooperate with the other nodes in the network for better communication. Therefore, the cooperativeness of the sensor nodes is measured based on communication links between the nodes over the specific time instant.

The communication links between the nodes are determined by the means of distributing the two beacon message distributions. The beacon messages are request (Req) and route replies (Rep) are shared among the sensor nodes. First, the sensor node SN_1 sends a request beacon message to other neighboring sensor nodes to identify the communication links.

$$SN_i \overset{Req}{\Longrightarrow} SN_j \ (6)$$

Where, the node SN_i sends route request (Req) beacon message to other sensor nodes SN_j in the network. The node SN_j sends the reply message Rep back to the node SN_i .

$$SN_j \overset{Rep}{\Longleftarrow} SN_i \ (7)$$

Where, node SN_j sends a reply message Rep to the sensor node SN_i. For each node compute the cooperative score values based on the received requests and responses.

$$CS = \frac{Rep_{\ rec}}{Req_{sent}} \quad (8)$$

Where, CS denotes a cooperative score of the each node based ratio of response received $Rep_{\ rec}$ from its neighbors and requests sends Req_{sent}. A higher cooperative score, close to 1, indicates that the sensor node is highly cooperative. This means the sensor node reliably responds to more requests from its neighbors, actively participates in data forwarding, and contributes positively to network operations. These kinds of nodes are considered reliable and are preferred for energy-efficient data transmission.

Conversely, a lower score value indicates that the sensor node is less cooperative. This suggests that the node frequently fails to respond to requests, drops requests. Nodes with low cooperation negatively impact the network's performance and decrease reliability. In this way, the cooperativeness of the particular sensor node is determined for secure data communication in WSN.

Followed by, the node trust value is estimated to improve security, reliability, and successful data transmission in WSN. A lightweight trust evaluation method is employed for decentralized WSN which measures the direct trust and indirect trust to identify the nodes as trusted or untrusted.

The direct trust values of the nodes are computed as a ratio of number of successful data transmission to the total number of data transmission, including both successful and unsuccessful data transmission. This value indicates the reliability and trustworthiness of node of the node. The direct trust value is mathematically expressed as follows,

$$T^{SN} = \left[\frac{S_{DT}}{S_{DT}+US_{DT}}\right] \quad (9)$$

Where, T^{SN} denotes a trust of sensor nodes, S_{DT} represents a successful data transmission, US_{DT} denotes an unsuccessful data transmission. With the estimated rust value, the direct trust and indirect trust is estimated as follows.

$$DT^{SN} = f_c * \sum(\vartheta_1 * T^{SN}) \quad (10)$$

$$IT^{SN} = \sum(\vartheta_2 * DT^{SN}) \quad (11)$$

$$T^{SN}_{total} = (\vartheta_3 * DT^{SN}) + (\vartheta_4 * IT^{SN}) \quad (12)$$

Where, DT^{SN} denotes a direct trust of the sensor node, IT^{SN} indicates a indirect trust of the sensor node, f_c denotes a confidence or normalization factor that scales the overall trust value, $\vartheta_1, \vartheta_2, \vartheta_3$ and ϑ_4 denotes a weight assigned to each interaction, T^{SN}_{total} denotes a total trust value of the sensor nodes.

The estimated energy cooperative score and trust values of the each node is formulated as follows,

$$M = \begin{bmatrix} E_{11} & CS_{11} & T_{1n} \\ E_{21} & CS_{22} & T_{2n} \\ \vdots & \vdots & \vdots \\ E_{m1} & CS_{m2} & T_{mn} \end{bmatrix} \quad (13)$$

Where,M indicates a vector of three different characteristics of the sensor nodes, each column indicates a characteristics of the sensor nodes Energy (E), cooperative score (CS) and trust (T) respectively.

The estimated vector consisting of three distinct characteristics of the sensor nodes is forwarded to the third hidden layer, where changepoint linear regression analysis is performed. This analysis identifies variations in the relationships among the input key characteristics by detecting transition points, enabling more accurate modeling of node behavior and improving decision-making in the network.

It is a machine learning technique used for analyzing the distinct characteristics of the sensor nodes and dependent variables i.e. target output.

$$IN = \beta_1 . M + c_1, if\ M < BP \quad (14)$$

$$LN = \beta_2 . M + c_2, if\ M > BP \quad (15)$$

Where, 'LN' represent the legitimate node and their different characteristics of the sensor nodes 'M' via regression coefficient 'β_1', 'β_2' and regression constants 'c_1', 'c_2' with respect to breakpoints 'BP' (i.e. threshold), IN symbolize the intruder nodes.

Based on the classification results, the error rate is measured based on squared difference between the actual and predicted output.

$$ERR = (Y_{AC} - Y_{PRE})^2 \quad (16)$$

Where, ERR denotes a classification error, Y_{AC} indicates the actual classification output, Y_{PRE} denotes the predicted output. In the fine-tuning phase, the deep learning model updates its hyperparameters to reduce the classification errors and increases the accuracy of node classification. The Gradient momentum function is employed to adjust the weights among the layers in MLP architectures.

$$Q_{t+1} = Q_t - \eta\, H_t \quad (17)$$

$$H_t = \gamma\, H_{t-1} + (1-\gamma)\frac{\partial ERR}{\partial W_t} \quad (18)$$

Where,Q_{t+1} indicates an updated weight, Q_t represents a current weight, η denotes a learning rate, '$\frac{\partial ERR}{\partial W_t}$' indicates a partial derivative of the classification error 'ERR' with respect to the current weight 'Q_t', γ indicates default value 0.9 . Based on the updated values, multiple weight vectors are generated. From these, the optimal weight vector is chosen using the Walrus Optimization algorithm, which increases the classification accuracy by minimizing errors.

The Metaheuristic Walrus Optimization algorithm is a nature-inspired technique designed based on foraging activities of walruses. In this algorithm, each walrus represents a number of weights.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue I Jan 2026- Available at www.ijraset.com

The advantage of Walrus Optimization algorithm provides the better performance in finding better quality solutions. The algorithm processed in three major phases namely exploration, migration, and exploitation to discover the optimal solution by the means of ranking process. The optimization process starts to perform the population of Walrus i.e. weights in a random manner.

$$Q_r = \begin{bmatrix} Q_1 \\ Q_2 \\ \vdots \\ Q_b \end{bmatrix} \quad (19)$$

Where, Q_r indicates 'b' population of weights. Followed by, fitness is estimated according to the error values.

$$fit(Q_r) = arg\ min\ ERR \quad (20)$$

Where $fit(Q_r)$ indicates a fitness for each weight, $arg\ min$ indicates an argument of minimal function, ERR represents an error rate. Subsequently, the current best weight is chosen from the population based on fitness.

$$Z = \begin{cases} fit(Q_r) > fit(Q_h)\ ; & select\ Q_r\ as\ best \\ Otherwise\ ; & Q_h\ as\ best \end{cases} \quad (21)$$

Where,Z represents current best selection outcomes, $fit(Q_h)$ denotes a fitness of the neighboring walrus,$fit(Q_r)$ indicates a fitness of one walrus. Accordingly, the highest fitness value is identified as the strongest walrus in the population. Subsequently, three distinct behaviors such as exploration, migration, and exploitation are carried out to effectively balance multiple objectives and guide the search toward the optimal solution.

1) Exploration

Exploration helps to maintain population diversity and increases the possibility of finding global optimal or near-optimal solutions than the local optima. The strongest walrus indicates the current best solution (best fitness function). Other walruses adjust their positions toward this best strongest walrus. Therefore, the position of other walruses gets adjusted as follows,

$$P\ (t+1) = P\ (t) + r.0.5|P_{best}(t) - J.P\ (t)| \quad (22)$$

Where, $P\ (t+1)$ represents an updated position of the walruses, $P\ (t)$ represents a current position of walruses, r represents a random numbers between [0, 1], $0.5|P_{best}(t) - J.P\ (t)|$ denotes a Jensen Shannon divergence between the current position '$P\ (t)$' and best position '$P_{best}(t)$', J represents the selected randomly between 1 or 2 and it is used to increase the algorithm's exploration ability.

2) Migration behaviors

The other behavior of walruses is the seasonal migration to stony seashores or temperatures increase during summer. In this behavior, each walrus moves toward the position of another randomly chosen walrus positioned in a various region. This migration behavior is mathematically expressed as follows,

$$P_M\ (t+1) = \begin{cases} P\ (t) + r.0.5|P_{best}(t) - J.P\ (t)|\ ; & if\ fit(P_{rand}(t)) > fit(P_i\ (t)) \\ P\ (t) + r.0.5|P\ (t) - P_{rand}(t)|\ ; & otherwise \end{cases} \quad (23)$$

Where, $P_M\ (t+1)$ represents a position of the other walruses in migration phase, $P_{rand}(t)$ indicates a position of another randomly selected walrus, r denotes a random number between 0 and 1 that controls the step size. j integers selected randomly between 1 or 2, $fit(P_{rand}(t))$ denotes a fitness of the randomly selected walrus, $fit(P_i\ (t))$ denotes a fitness of the current selected walrus.

3) Exploitation

During this behavior, walruses are exposed to risks from predators such as polar bears and killer whales. In this behavior, exploitation is the process of altering the solutions in promising areas according to the current knowledge, focusing on achieving the best result by finding the neighborhood of known best solutions. The position updating process of the walruses in exploitation is expressed as follows,

$$P_E\ (t+1) = P\ (t) + \left(U_b + (L_b - r.L_b)\right) \quad (24)$$

©IJRASET: All Rights are Reserved

Where, $P_E\ (t+1)$ indicates a updated position, $P\ (t)$ represents current location of the walrus, L_b denotes a local bounds, U_b represents a upper bounds for the search range around the walrus, r indicates a random number between 0 and 1. Finally, the algorithm verifies the new position along with previous position according to

$$P\ (t) = \begin{cases} fit\ (P_E\ (t+1)) > fit\ (P\ (t)) \ ; & return\ P_E\ (t+1)\ is\ optimal \\ Otherwise \ ; & return\ P\ (t)\ is\ optimal \end{cases} \quad (25)$$

If the fitness of new position '$P_E\ (t+1)$' is greater than the current best '$P\ (t)$ it may replace the newly selected best-known position $P_E\ (t+1)$ as an optimal. This process continues until the maximum number of iterations gets achieved. Finally, the optimal position of walrus (i.e., optimal weight) is making small changes in the direction that minimizes the error. This process helps refine learned reduce prediction errors, and improve overall accuracy of the model. Finally, the accurately classified results are generated at output layer with sigmoid activation function.

$$Y\ =\ A_{sigmoid}(h(t)) \quad (26)$$

Where, 'Y' denotes a final binary classification output, '$h(t)$' represents the hidden layer output, '$A_{sigmoid}$' represents the sigmoid activation function in output layer for binary classification output. Finally, the data communication is carried out through legitimate sensor nodes to increase the security.

// Algorithm 1: Linear Regressive Momentum Optimized Dense neural Network
Input: Number of sensor nodes '$SN_1, SN_2, SN_3, \ldots, SN_n$, Environmental data packets $DP_1, DP_2, DP_3, \ldots . DP_n$
Output: Security of data transmission
Begin
Step 1: Number of sensor nodes '$SN_1, SN_2, SN_3, \ldots, SN_n$ and Environmental data packets --- input layer
Step 2: input of SN_n s given to input layer of MLP
Step 3: Compute the weighted sum using (1)
Step 4: For each sensor node SN_i --- Hidden layer 1
Step 5: Compute the residual energy using (5)
Step 6: End for
Step 7: For each sensor node --- Hidden layer 2
Step 8: Compute the cooperative score 'CS' using (8)
Step 9: Compute the total trust value of sensor nodes T_{total}^{SN} using (12)
Step 10: End for
Step 11: Formulate the vector of different characteristics of sensor nodes 'M' using (13)
Step 12: If (M' $> BP$) then--- Hidden layer 3
Step 13: sensor node is classified as legitimate
Step 14: else
Step 15: sensor node is classified as intruder
Step 16: End if
Step 17: Obtain classes of sensor nodes
Step 18: For each classification result
Step 19: Measure the classification error ' ERR using (16)
Step 20: Update the weights using (17) (18)
Step 21: End for
Step 22: Initialize the population of the weights using (19)
Step 23: For each weight 'Q'
Step 24: Evaluate the fitness using equation (20)
Step 25: End for
Step 26: While ($T\ <\ T_{max}$) do
Step 27: if ($fit(Q_r) > fit(Q_h)$)then
Step 28: Select the current best weight
Step 29: End if
Step 30: for each weight in population do

Step 31: if the exploration phase then
Step 32: Update the positions '$P\ (t+1)$' using (22)
Step 33: Else if Migration phase then
Step 34: Update the positions '$P_M\ (t+1)$' using (23)
Step 35: End if
Step 36: End for
Step 37: Calculate new position in the neighborhood of the walrus using (24)
Step 38: if $\left(fit\left(P_E\ (t+1)\right) > fit\ \left(P\ (t)\right)\right)$ then
Step 39: $P_E\ (t+1)$ considered as best optimal solution
Step 40: else
Step 41: $P\ (t)$ considered as optimal solution
Step 42: End if
Step 43: Increment t= t+1
Step 44: Go to step 8
Step 45: End While
Step 46: Return best optimal according to fitness
Step 47: Obtain accurate node classification results at output layer using (26)
Step 48: Perform secured data transmission through legitimate sensor nodes
End

Algorithm 1 describes the step by step process of secure data transmission between sensor node and sink node in WSN. The Dense neural network is used as a feed forward deep learning model to classify the sensor nodes into legitimate or intruder nodes. The input i.e. sensor nodes are given to the input layer. In the hidden layer, the nodes residual energy, trust value, cooperativeness is calculated. After that, the changepoint linear regression is employed for classifying the sensor node as legitimate or intruder nodes by setting the break point or threshold. After the classification, the training error rate is computed. Based on the error rate, the weight values get updated accordingly. Afterward, the weight parameters are initialized and optimized using a population-based walrus optimization. During this process, the fitness of each candidate weight solution is iteratively estimated, and the best-performing solutions are chosen to update the weight positions. If a newly updated weight achieves better fitness, it replaces the previous weight. Otherwise, the existing weight gets retained. This optimization process continues until the predefined maximum number of iterations is reached. In deep learning models, the optimal weight values guide the backpropagation to minimize the error function. Finally, the output layer produces the accurate classification results with reduced error, thereby enhancing the overall detection performance. The data transmission is performed through the legitimate node for attaining high security.

IV. SIMULATION SETUP

In this section, simulation of three different methods namely the proposed LiRMO-DenseNet model, an existing method referenced as QS-BAT [1], and MLSRP [2] are implemented using the NS3 simulator. A total of 500 sensor nodes are deployed within a square area of 1100 m × 1100 m. The Random Waypoint mobility model is adopted to support energy-efficient secure routing in the wireless sensor network (WSN). The simulation duration is set to 100 seconds. To further enhance energy efficiency and ensure secure data communication, the Dynamic Source Routing (DSR) protocol is utilized. The simulation parameters and their corresponding values are summarized in Table 1.

Table 1 Simulation Parameters

Simulation parameters	Value
Simulator	NS3
Network area	1100m * 1100m
Number of sensor nodes	50, 100, 150, 200…500
Number of data packets	100, 200, 300, ….1000

Protocol	DSR
Simulation time	100sec
Mobility model	Random Way Point model
Nodes speed	0-20m/s
Communication range of a sensor nodes	30m
Number of runs	10

A. Simulation Implementation Results

This section explains the various processes involved in the LiRMO-DenseNet model,with the support of illustrative screenshots. Initially, 50 sensor nodes are randomly distributed over a square area of $1100 \times 1100\, m^2$.

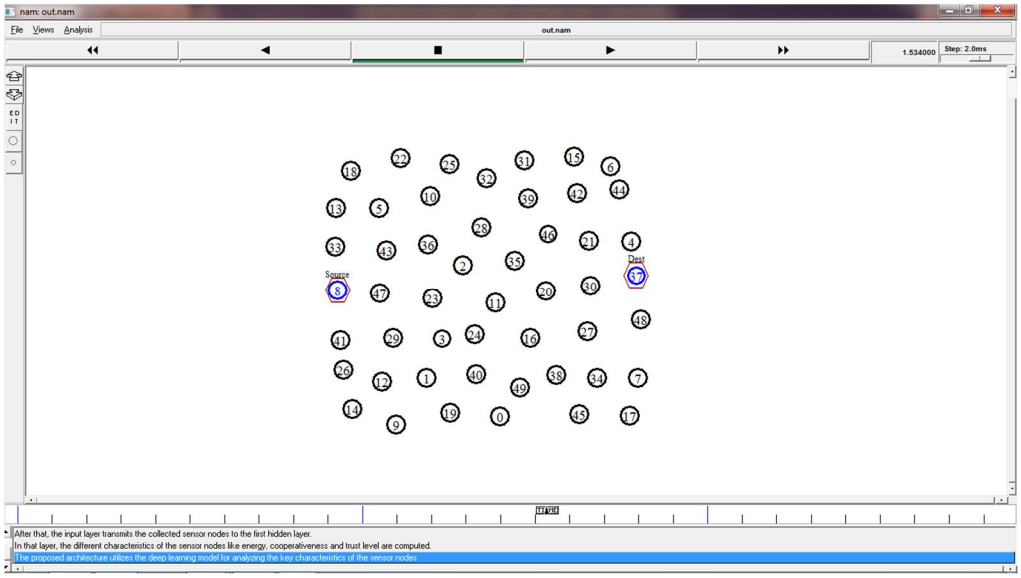


Figure 3 sensor nodes deployments

Following the deployment of sensor nodes within the designated network area, energy, trust and cooperativeness of sensor nodes are measured as illustrated in Figure 4.

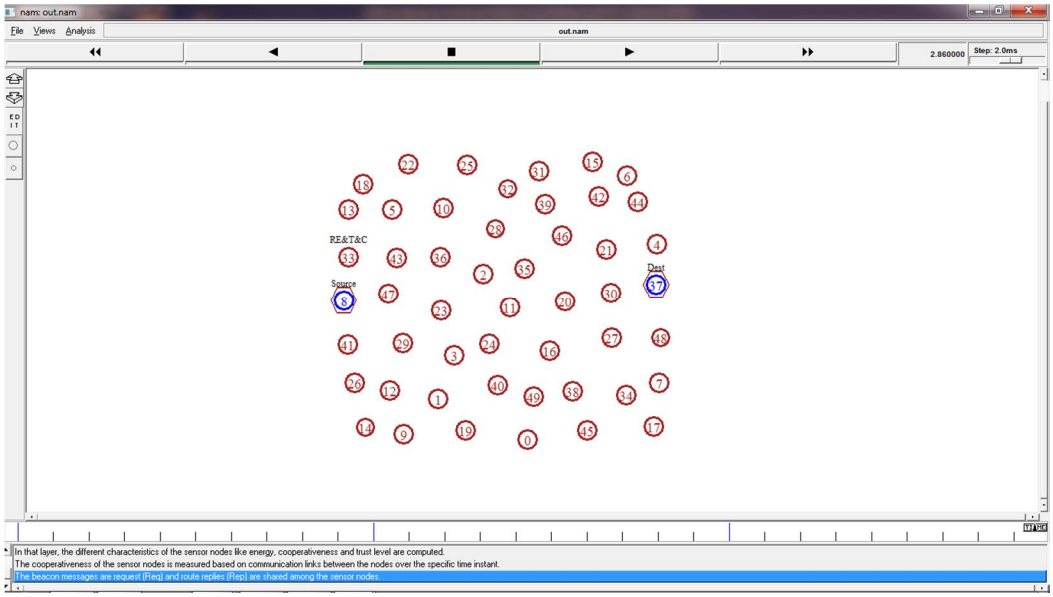


Figure 4 sensor nodes energy, trust and cooperativeness of sensor nodes measurements

After measuring the characteristics of sensor nodes, Change point linear regression analysis is carried out in dense neural network model for classifying the legitimate and intruder sensor nodes in WSN.

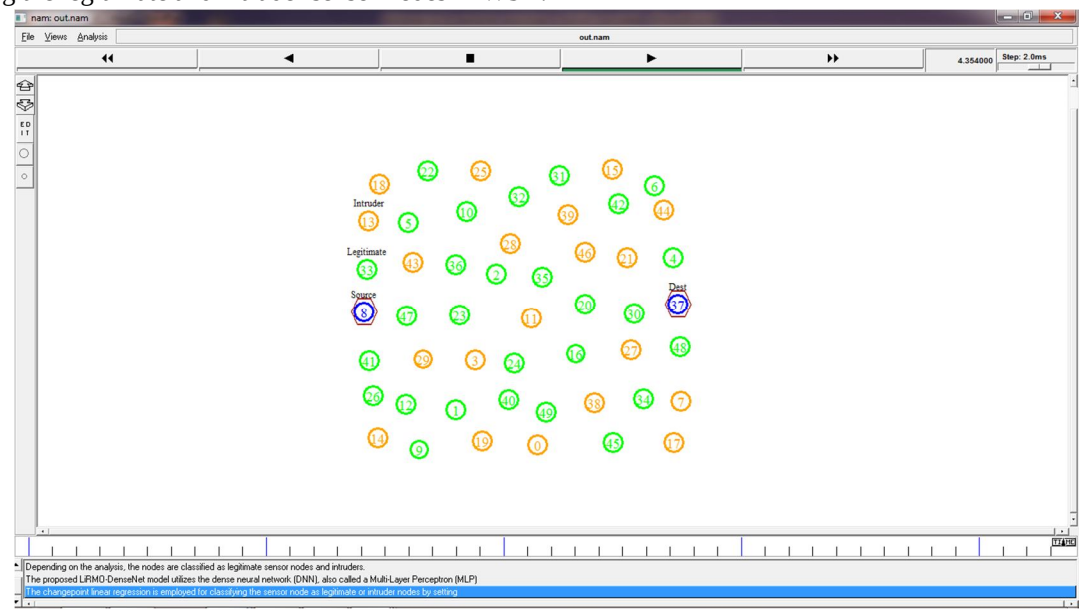


Figure 5 sensor nodes classification

Figure 5 demonstrates 50 sensor nodes randomly deployed within the network area. The nodes are represented using different colors to indicate their roles and status. Green nodes denote legitimate sensor nodes, while orange nodes represent intruder nodes identified during the detection process.

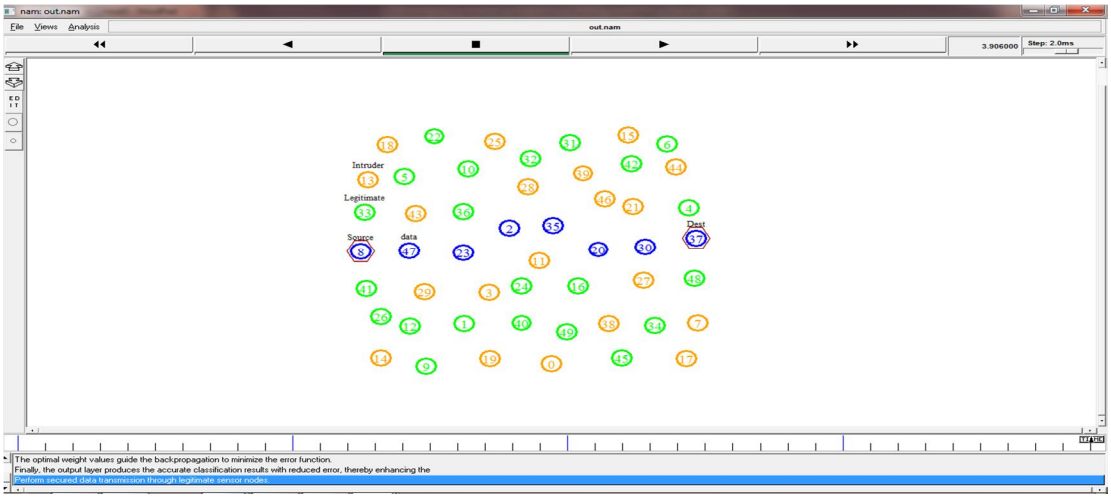


Figure 6 data transmission via legitimate sensor node

The figure 6 illustrates the data transmission process after intrusion detection in the WSN. In this scenario, legitimate nodes are shown in green, while intruder nodes are indicated in orange. The source node initiates data transmission through the legitimate nodes for secure data delivery and supports reliable routing while mitigating security threats within the network.

V. PERFORMANCE RESULTS AND DISCUSSION

This section offers a relative analysis of LiRMO-DenseNet model by comparing it with established state-of-the-art methods, namely QS-BAT [1], and MLSRP [2]. The performance evaluation uses metrics such as including accuracy, precision, recall, F1 score, data transfer security rate, throughput and end to end delay. The performance of LiRMO-DenseNet model is compared to existing model with respect to these metrics is illustrated through tables and graphical representations.

A. Performance Comparison Analysis of Accuracy

It refers to the ratio of correctly classified the sensor nodes as legitimate or intruders to the total number of sensor nodes. The corresponding mathematical formula for accuracy is expressed as follows,

$$Accuracy = \left(\frac{TP+TN}{TP+TN+FP+FN}\right) * 100 \qquad (27)$$

Where TP (True Positive) represents the number of correctly identified legitimate nodes, TN (True Negative) denotes the number of correctly identified intruder nodes, FP (False Positive) refers to intruder nodes incorrectly classified as legitimate nodes, and FN (False Negative) represents legitimate nodes incorrectly classified as intruder nodes. Accuracy is measured as a percentage (%).

Table 2 comparison analysis of accuracy

Number of sensor nodes	Accuracy (%)		
	Proposed LiRMO-DenseNet	Existing QS-BAT [1]	Existing MLSRP [2]
50	94	90	86.27
100	96.32	92.36	89.23
150	97.23	91.56	90.05
200	96.56	92.33	89.52
250	96.41	91.56	90.05
300	96.78	92.63	91.23
350	97.21	93.22	91.63
400	98.1	93.45	91.44
450	97.26	93.22	91.03
500	97.22	92.45	90.23

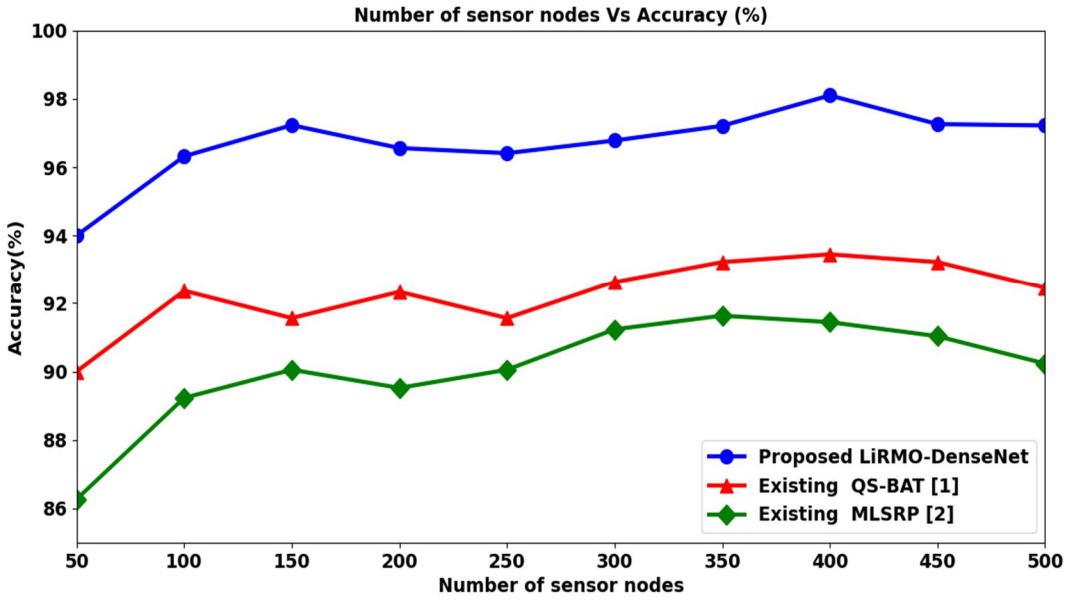


Figure 7 graphical illustration of accuracy

Figure 7 shows a comparative examination of accuracy including the proposed LiRMO-DenseNet model is evaluated by comparing it against existing methods, namely QS-BAT [1], and MLSRP [2]. The analysis measures accuracy of intruder detection based on sensor nodes with various ranging from 50 to 500. Among three methods, the LiRMO-DenseNet model consistently outperforms the other approaches in terms of achieving higher accuracy.

For instance, with a 50 sensor nodes, LiRMO-DenseNet model achieves an accuracy of 94%. In comparison, [1] reaches 90%, [2] records 86.27%, respectively. Subsequently, various performance results were observed with respect to various counts of input sensor nodes. Finally, the observed results of LiRMO-DenseNet model are compared to results of existing methods. The average of ten results illustrates an improvement in accuracy of approximately 5%, and 7% when compared to [1], [2], respectively. This performance improvement is chiefly achieved to the integration of dense feed forward neural network architecture. This architecture helps to identify sensor devices that have higher residual energy, cooperative score and trust value by applying the changepoint linear regression for secure data transmission, resulting overall accuracy of legitimate and intruder node is significantly improved.

B. Performance comparison analysis of precision

Precision is measured as the ratio of correctly predicted positive instances (true positives) to the total number of instances predicted as positive, which includes both true positives and false positives. The formula for precision is expressed as follows

$$\boldsymbol{Precision} = \left(\frac{TP}{TP+FP}\right) * \mathbf{100} \qquad (28)$$

Where, TP represents the true positive, FP indicates the false positive.

Table 3 comparison analysis of precision

Number of sensor nodes	Precision (%)		
	Proposed LiRMO-DenseNet	Existing QS-BAT [1]	Existing MLSRP [2]
50	94.87	92.30	89.74
100	96.23	93.36	90.33
150	96.11	93.26	91.06
200	96.22	93.44	91.45
250	96.25	93.56	91.66
300	96.36	93.23	91.41
350	96.88	93.56	90.63
400	97.11	93.36	91.45
450	96.32	92.66	91.55
500	96.63	93.05	91.36

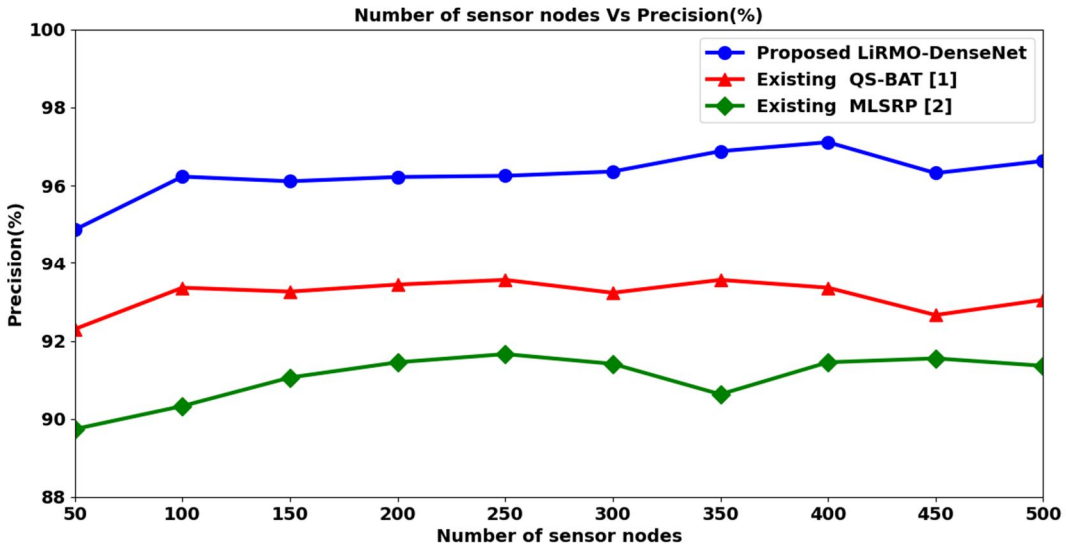


Figure 8 graphical illustration of precision

Figure 8 presents a comparison of precision across varying numbers of sensor nodes ranged from 50 to 500. In the chart, the x-axis represents the number of sensor nodes, and the y-axis indicates the corresponding precision values in intruder node classification. Among the three methods, LiRMO-DenseNet model achieves the highest precision, outperforming the other existing approaches. For example, when using 50 sensor nodes, the LiRMO-DenseNet model achieved a precision of 94.87%, while the existing methods [1] and [2] achieved 92.30% and 89.74% respectively. On average, LiRMO-DenseNet model demonstrates an improvement in precision of approximately 3% over method [1] and around 6% over method [2]. This improvement is achieved due to the integration of dense neural learning techniques, which incorporate the walrus optimization algorithm for fine-tuning the sensor node classification results. By iteratively tuning the deep learning model hyperparameters, the system increases its learning process, directing to high true positives and less false positives, thereby enhancing the precision performance in sensor node classification.

C. Performance Comparison Analysis of Recall

It also known as sensitivity, evaluates the model effectiveness in correctly identifying intruder and malicious node. It is measured by dividing the number of true positive predictions by the total of true positives and false negatives.

$$Recall = \left(\frac{TP}{TP+FN}\right) * 100 \quad (29)$$

Where, TP indicates the true positive, FN represents the false negative.

Table 3 comparison analysis of recall

Number of sensor nodes	Recall (%)		
	Proposed LiRMO-DenseNet	Existing QS-BAT [1]	Existing MLSRP [2]
50	97.36	94.73	92.10
100	98.33	96.36	93.23
150	98.11	96.11	93.25
200	98.36	96.05	93.25
250	97.98	96.02	93.63
300	98.23	96.13	93.47
350	97.86	96.16	93.65
400	98.15	96.02	93.45
450	98.11	95.68	93.85
500	98.12	95.33	93.41

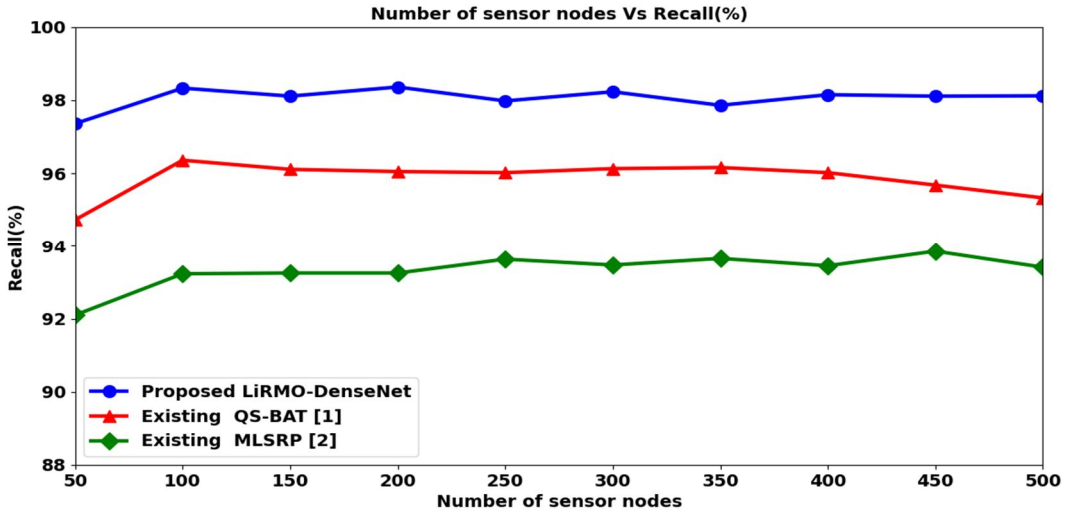


Figure 9 graphical illustration of recall

Figure 9 portrays a performance evaluation of recall with respect to the number of sensor nodes deployed in the WSN. The LiRMO-DenseNet model exposes higher recall compared to the existing approaches [1] and [2]. For instance, with 50 sensor nodes, LiRMO-DenseNet model achieved a recall of 97.36%, while methods [1] and [2] observed 94.73% and 92.10%, respectively. After reaching the ten performance runs, the average recall rate of LiRMO-DenseNet model improved by approximately 2% compared to [1] and 5% compared to [2]. The improved recall performance of the LiRMO-DenseNet model is achieved owing to the fine-tuning process employed within the dense neural network architecture. By utilizing a fine-tuning process, the model minimizes the classification error between predicted and actual outcomes through hyperparameter adjustment using the walrus optimization algorithm. This iterative process continues until the classification error gets minimized, resulting in fewer false negative results and increase in true positives.

D. Performance Comparison Analysis of F1 Score

It also called as F-measure refers to the harmonic mean of precision as well as recall. It is mathematically calculated using following expression.

$$F1 - Score = 2 * \left(\frac{Precion * Recall}{Precion + Recall}\right) \quad (30)$$

Table 3 comparison analysis of recall

Number of sensor nodes	F1 score (%)		
	Proposed LiRMO-DenseNet	Existing QS-BAT [1]	Existing MLSRP [2]
50	96.09	93.49	90.90
100	97.26	94.83	91.75
150	97.09	94.66	92.14
200	97.27	94.72	92.34
250	97.10	94.77	92.63
300	97.28	94.65	92.42
350	97.36	94.84	92.11
400	97.62	94.67	92.43
450	97.20	94.14	92.68
500	97.36	94.17	92.37

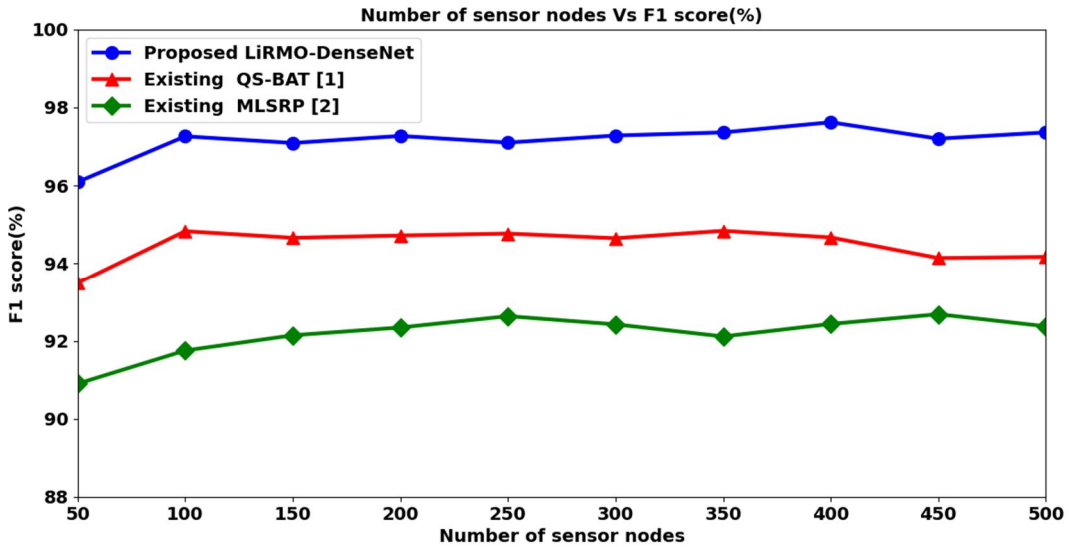


Figure 10 graphical illustrations of F1 score

Figure 10 illustrates a performance comparison of F1 scores for different number of sensor nodes ranging from 50 to 500. The results confirm that the proposed LiRMO-DenseNet model constantly outperforms conventional models in terms of achieving high F1 score. Each method was analyzed over ten various results to obtain consistent F1 measurements. The analysis exposes that LiRMO-DenseNet model achieves superior F1 score performance across all simulations. The average of ten results indicates that the LiRMO-DenseNet model showed an improvement of F1 score approximately 5% over method [1] and 3% over method [2]. This enhanced performance is owing to the efficient implementation of the dense neural network, which enhances the F1 score by balancing effects of precision as well as recall, leading to more accurate and consistent sensor node classification.

E. Performance Comparison of Data transfer security rate

Data transfer security Performance measures the effectiveness of the proposed approach in safeguarding transmitted data against intruder node access in a WSN. It quantifies reliable data packets are delivered without being altered by intruder nodes. The metric is computed as the ratio of secure transmissions to the total number of transmissions. A higher Data Security Performance value indicates stronger protection, and improved reliability of the secure data communication process within the network.

$$DTS = \sum_{j=1}^{m} \left[\frac{DPCD}{DP_j}\right] * 100 \quad (31)$$

Where DTS refers to a Data transfer Security rate, $DPCD$ symbolizes the data packets correctly delivered at the sink node and $DP_j\ sent$ indicates a data sent. The ratio is measured in terms of percentage (%).

Table 3 comparison analysis of Data Security rate

Number of data packets	Data transfer Security rate (%)		
	Proposed LiRMO-DenseNet	Existing QS-BAT [1]	Existing MLSRP [2]
100	96	93	91
200	96.23	92.36	90.05
300	96.74	92.23	90.63
400	96.36	92.15	90.36
500	97.05	93.05	91.22
600	96.88	92.32	90.65
700	96.11	92.41	90.41
800	96.07	92.33	90.65
900	96.15	92.41	90.05
1000	96.12	92.36	90.66

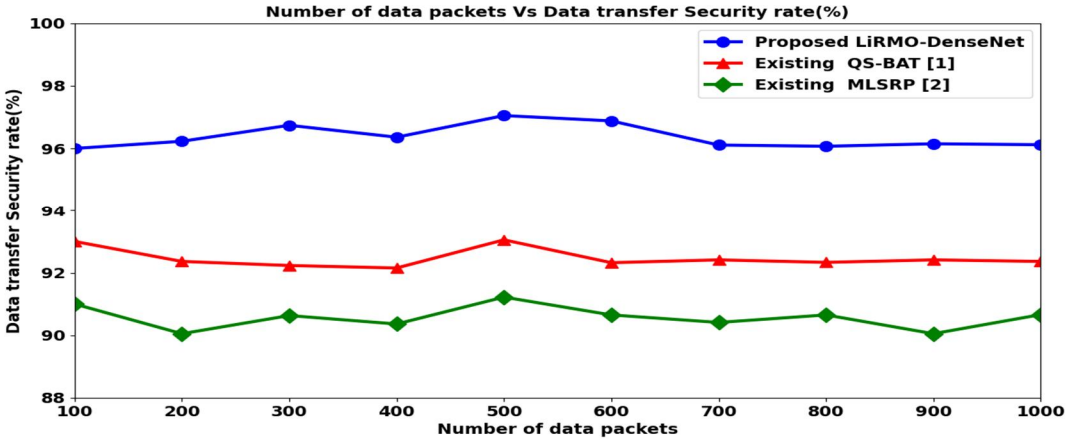


Figure 11 graphical illustrations of Data transfer Security rate

Figure 11 demonstrates the performance comparison of data transfer security rate using four different methods namely the proposed LiRMO-DenseNet model is evaluated by comparing it against existing methods, namely QS-BAT [1], and MLSRP [2]. In the figure, the x-axis represents the number of data packets, ranging from 100 to 1000, while the y-axis shows the corresponding data transfer security rate. Among all the three methods, LiRMO-DenseNet model consistently achieves superior performance. For example, when considering 100 data packets to be transmitted, the LiRMO-DenseNet model records a data transfer security rate of 96%, whereas [1], [2] achieved data transfer security rate rates of 93%, and 91%, respectively. This assessment was conducted across ten various data volumes, and the results demonstrate a clear improvement. The LiRMO-DenseNet model maintains higher data transfer security rate in all cases. The average of ten results indicates that the LiRMO-DenseNet model outperforms the existing techniques by approximately 4% compared to [1], 6% compared to [2]. The improved performance of LiRMO-DenseNet model is achieved due to the integration of a dense neural network model. This deep learning architecture determined the legitimate and intruder nodes by the means of energy and cooperativeness and trust. Finally, the secure data transmission is carried out via legitimate sensor nodes, thereby enhancing the data transfer security.

F. Performance Comparison of Throughput

It measured as the rate of successful data transmission over a communication network within a specified time period. It is measured in bits per second (bps). The formula for calculating he throughput is measured as follows,

$$THP = \left[\frac{Succ_Trans_data\ packet\ (bits)}{time\ (s)}\right] \quad (32)$$

Where, THP indicates a throughput, $Succ_Trans_data\ packet\ (bits)$ denotes a successful transmission of data packets in bits in one seconds (Bps).

Table 3 comparison analysis of Data Security rate

Data packet size (KB)	Throughput(bps)		
	Proposed LiRMO-DenseNet	Existing QS-BAT [1]	Existing MLSRP [2]
100	226	196	163
200	326	288	216
300	485	405	323
400	596	489	411
500	688	612	532
600	865	711	622
700	1123	936	823
800	1325	1163	986
900	1532	1325	1163
1000	1863	1532	1263

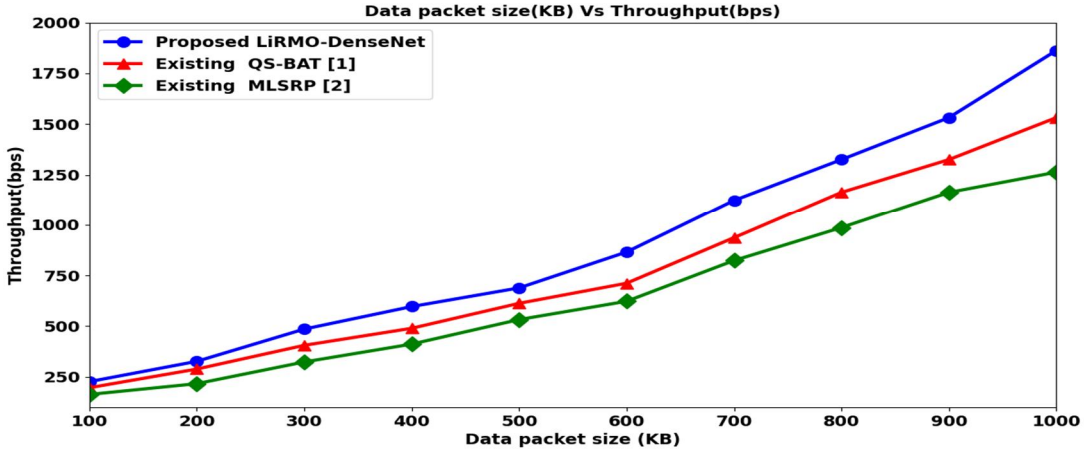


Figure 12 graphical illustrations of throughput

Figure 12 illustrates the graphical examination of throughput across three various methods LiRMO-DenseNet model is evaluated by comparing it against existing methods, namely QS-BAT [1], and MLSRP [2]. The horizontal axis represents size of data packets ranging from 100KB to 1000KB, while the perpendicular axis demonstrates the performance of throughput. Among the different approaches, LiRMO-DenseNet model consistently reveals higher throughput of successful data transmission. In initial iteration, 100KB of data being transmitted in sender node, the LiRMO-DenseNet model achieves a 226bps of throughput. In comparison, methods [1] and [2] recorded throughput of 196bps and 163bps, respectively. This assessment was reiterated across numerous runs, and the averages of ten results were considered for the final classification performance. The overall result indicates that LiRMO-DenseNet model outperforms the existing methods [1] [2], showing improvement of throughput approximately 18% and 40%. The performance enhancement is achieved by integrating the dense feed forward neural network. This network strategy facilitates the identification of the most suitable legitimate sensor nodes by evaluating parameters such as high residual energy, cooperativeness and trust value. As a result, data transmission becomes more efficient, leading to improved overall throughput in WSNs.

G. Performance Comparison of End to end delay

It is a key performance metrics that measures the amount of time it takes for data packets travelled from sender to sink node across a network. The formula for calculating the end to end delay is expressed as follows,

$$E2ED = T_j(R) - T_j(T) \quad (33)$$

Where, $E2ED$ denotes an End to end delay, $T_j(R)$ denotes a time of j^{th}data packet received at the sink node, $T_j(T)$ denotes a time of j^{th}data packet transmitted from sender. It is measured in milliseconds (ms).

Table 3 comparison analysis of End to end delay

Number of data packets	End to end delay (ms)		
	Proposed LiRMO-DenseNet	Existing QS-BAT [1]	Existing MLSRP [2]
100	11.8	13.5	15.6
200	12.5	15.2	18.3
300	13.4	16.4	19.4
400	15.6	18.2	20.5
500	18.7	20.5	22.6
600	20.9	22.3	25.4
700	23.6	26.1	28.4
800	26.5	28.4	30.2
900	30.2	32.3	34.7
1000	32.6	35.8	37.2

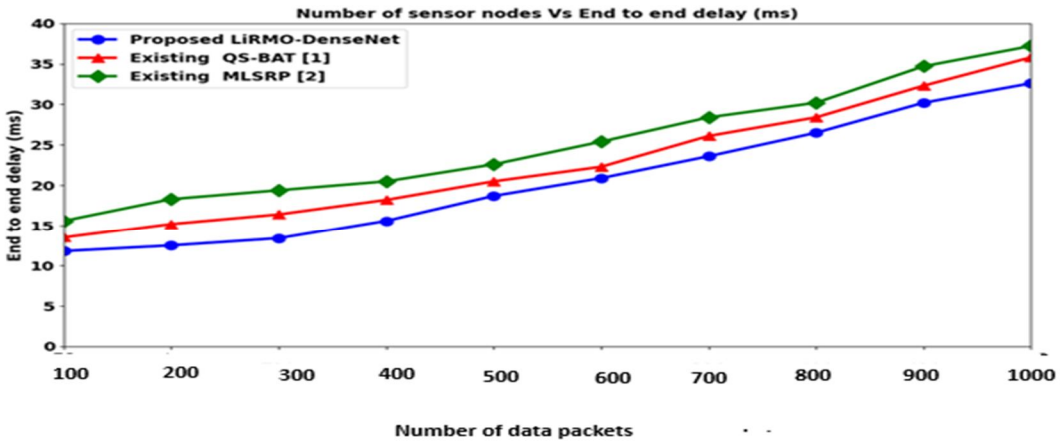


Figure 13 graphical illustrations of End to end delay

Figure 13 presents a performance assessment of end to end delay in relation to the number of data packets transmitted from the source node to sink. The findings reveal that, across all three methods analyzed, end to end delay increases as the data packet volume rises. However, the LiRMO-DenseNet model consistently demonstrates a significant reduction in transmission delay compared to the traditional approaches in [1] and [2]. For example, when 100 data are transmitted, the LiRMO-DenseNet model records a delay of 11.8 ms while the methods in [1] and [2] demonstrate delay of 13.5ms and 15.6ms, respectively. Throughout the range of increased data volumes, the LiRMO-DenseNet model achieves an average delay reduction of approximately 11% and 20% in comparison to the existing techniques. This improvement is largely achieved due to selecting the energy efficient sensor nodes to improve the overall efficiency of data transmission within the network. This approach increases the data transmissions speed, reduces communication overhead, and significantly lowers transmission delay.

H. Case Studies

In this section, the practical application of LiRMO-DenseNet model is analyzed to demonstrate its effectiveness and adaptability. These case studies highlight the proposed LiRMO-DenseNet model optimizes routing decisions under diverse network conditions by intelligently considering factors such as energy efficiency and security.

In order to conduct the case scenario, Healthcare_IOT_Data is collected from the https://www.kaggle.com/datasets/ziya07/healthcare-iot-data. This dataset represents sensor readings collected from wearable devices in an IoT-enabled healthcare environment and is used to evaluate secure data transmission in patient monitoring scenarios. It captures real-time physiological parameters such as body temperature, blood pressure, and heart rate, along with device-related attributes including sensor identity, timestamps, and battery levels. Each record is associated with a unique patient and sensor, enabling continuous health assessment and comparison against predefined target values for vital signs and health status. The inclusion of battery-related information supports energy-aware communication, which is critical for maintaining reliable and uninterrupted data transmission. In the context of secure healthcare applications, this dataset facilitates the analysis of sensitive patient data are transmitted efficiently and securely to healthcare providers while ensuring data security, reliability, and privacy in IoT-based remote monitoring systems.

VI. CONCLUSION

The paper introduces a novel approach called the LiRMO-DenseNet model, designed to achieve energy-efficient and secure data transmission in WSN. The proposed approach starts with the deployment of multiple sensor nodes across the large scale sensor network, followed by the application of a dense neural network that categorizes the nodes into legitimate or intruder according to their residual energy, trust and node cooperativeness. To further improve the classification accuracy performance, walrus optimization algorithm is employed. This optimization mechanism effectively minimizes error rate during sensor node classification. The effectiveness of the proposed LiRMO-DenseNet model is validated through extensive simulations using key performance metrics such as accuracy, precision, recall, F1 score, data transfer security, throughput, and end to end delay. The simulation results clearly designate that the LiRMO-DenseNet model outperforms existing approaches by achieving superior data transfer security, throughput and transmission success while considerably lowering delay when compared to conventional methods.

REFERENCES

[1] K. Vinotha , P. Eswaran, “Quantum inspired hyperparameter optimization for enhanced deep learning based intrusion detection in wireless sensor networks”, Systems and Soft Computing, Elsevier, Volume 8, June 2026, Pages 1-12. https://doi.org/10.1016/j.sasc.2025.200431

[2] [16] Edeh Michael Onyemaa, S. Kanimozhi Sugunac, B. Sundaravadivazhagand , Rutvij H. Jhaverie , Ugwuja Nnenna Estherf , Edeh Chinecherem Deborahg , K. Shantha Kumari, “A secure routing protocol for improving the energy efficiency in wireless sensor network applications for industrial manufacturing”, Next Energy, Elsevier, Volume 7, 2025, Pages 1-8. https://doi.org/10.1016/j.nxener.2024.100219

[3] S. Ramachandra, M. Baskar, “Real-time multi-level trust-based secure routing for improved QoS in WSN using blockchain”, Results in Engineering, Elsevier, Volume 26, 2025, Pages 1-10. https://doi.org/10.1016/j.rineng.2025.104732

[4] S. Ambareesh, Pundalik Chavan, S. Supreeth, Rajesh Nandalike, P. Dayananda & S. Rohith, “A secure and energy-efficient routing using coupled ensemble selection approach and optimal type-2 fuzzy logic in WSN”, Scientific Reports, volume 15, 2025, Pages 1-24. https://doi.org/10.1038/s41598-024-82635-w

[5] Rahul Priyadarshi, Ravi Ranjan Kumar, Rakesh Ranjan & Padarti Vijaya Kumar, “AI-based routing algorithms improve energy efficiency, latency, and data reliability in wireless sensor networks”, Scientific Reports, volume 15, 2025, Pages 1-19. https://doi.org/10.1038/s41598-025-08677-w

[6] Prafull Goswami, Tayyab Khan, Vinay Pathak & Abdulatif Alabdultif, “Machine learning based dynamic trust estimation framework for Securing wireless sensor networks”, Scientific Reports, volume 15, 2025, Pages 1-19. https://doi.org/10.1038/s41598-025-19768-z

[7] R Barath Ramesh, S. John Justin Thangaraj, G. Mary Amirtha Sagayee, K. Saravanan, “Detection and prevention in WSN security framework using deep learning against black hole and wormhole attacks”, Ain Shams Engineering Journal, Elsevier, Volume 16, Issue 10, 2025, Pages 1-13. https://doi.org/10.1016/j.asej.2025.103624

[8] Poornima Poojar, Muhibur Rahman, Nagaraj Basavaraj Patil, "Energy Efficient and Secure Clustering and Routing Using Multi-Objective Trust Aware Adaptive Oscillation Weight Cheetah Optimization Algorithm", International Journal of Intelligent Engineering and Systems, Volume 18, Issue 7, 2025, Pages 210-223. DOI: 10.22266/ijies2025.0831.15

[9] Shaha Al-Otaibi, Sarra Ayouni, Nadeem Sarwar, Asma Irshad & Faizan Ullah, "AI-driven intrusion detection and lightweight authentication framework for secure and efficient medical sensor networks", Scientific Reports , 2025, Pages 1-27. https://doi.org/10.1038/s41598-025-31981-4

[10] Santosh Anand, Anantha Narayanan V, "Addressing Rogue Nodes and Trust Management: Leveraging Deep Learning-Enhanced Hybrid Trust to Optimize Wireless Sensor Networks Management", Journal of Robotics and Control (JRC), Volume 6, Issue 2, 2025, Pages 846-861. DOI: 10.18196/jrc.v6i2.25600

[11] Hanadi Ahmad Simmak, Ahmed A El-Douh, Tareef S Alkellezli, Rabih Sbera, Darin shafek, Ahmed Abdelhafeez, "Improving the Routing Security in Wireless Sensor Networks using Neutrosophic Set and Machine Learning Models", Neutrosophic Sets and Systems, Volume 87, Pages 900-909. https://fs.unm.edu/nss8/index.php/111/article/view/6597

[12] Sarvenaz Sadat Khatami, Mehrdad Shoeibi, Reza Salehi and Masoud Kaveh, "Energy-Efficient and Secure Double RIS-Aided Wireless Sensor Networks: A QoS-Aware Fuzzy Deep Reinforcement Learning Approach", Journal of sensor and actuator network, Volume 14, Issue 1, 2025, Pages 1-29.https://doi.org/10.3390/jsan14010018

[13] Shaik Shafiuddin, Konda Hari Krishna, "TrustRIDR-Net: A Hybrid Trust-Aware Routing Framework Using RFO and DRL for Scalable IoT Networks", Engineering, Technology & Applied Science Research, Volume 15, Issue 5, 2025, Pages 27421-27429. https://doi.org/10.48084/etasr.12294

[14] Vikas, Charu Wahi, Bharat Bhushan Sagar and Manisha Manjul, "Trusted Energy-Aware Hierarchical Routing (TEAHR) for Wireless Sensor Networks", Sensors, Volume 25, Issue 8, 2025, Pages 1-36. https://doi.org/10.3390/s25082519

[15] G. Nagarajan, R.I. Minu, Meena Devi R, T. Samraj Lawrence, Sajith P J , M. Viju Prakash, "Eco-conscious multi-factor authentication protocols for energy-aware wireless networks", Results in Engineering, Elsevier, Volume 28, 2025, Pages 1-14. https://doi.org/10.1016/j.rineng.2025.107807

[16] Mohammad Bilal J, D. Suresh & R. Karthikeyan, "Sleep-wakeup based secure multipath routing in wsn using fennec fox optimized deep learning framework", Scientific Reports, volume 16, 2026, Pages 1-27. https://doi.org/10.1038/s41598-025-30622-0

[17] Radha Raman Chandan , Hemalatha Thanganadar, Upendra Dwivedi, Surendra Kumar Shukla, Shreyas Pagare, Navruzbek Shavkatov, "Energy-efficient multi factor authentication protocols in sustainable security for wireless networks using machine learning algorithm", Results in Engineering, Elsevier, Volume 28, 2025, Pages 1-8. https://doi.org/10.1016/j.rineng.2025.107196

[18] Priyanshu Sinha, Dinesh Sahu, Shiv Prakash, Rajkumar Singh Rathore, Pratibha Dixit, Vivek Kumar Pandey & Iryna Hunko, "An efficient data driven framework for intrusion detection in wireless sensor networks using deep learning", Scientific Reports, volume 15, 2025, Pages 1-25. https://doi.org/10.1038/s41598-025-12867-x

[19] Mohamed Loughmari, Anass El Affar, "A lightweight machine learning approach for denial-of-service attacks detection in wireless sensor networks", International Journal of Electrical and Computer Engineering (IJECE), volume 15, Issue 2, 2025, Pages. 2089-2097 DOI: 10.11591/ijece.v15i2.pp2089-2097

[20] Kenan Honore Robacky Mbongo, Kanwal Ahmed, Orken Mamyrbayev, Guanghui Wang, Fang Zuo, Ainur Akhmediyarova , Nurzhan Mukazhanov and Assem Ayapbergenova, "Conv1D-GRU-Self Attention: An Efficient Deep Learning Framework for Detecting Intrusions in Wireless Sensor Networks", Future Internet, Volume 17, Issue 7 , 2025, Pages 1-20. https://doi.org/10.3390/fi17070301

[21] Ra'ed M. Al-Khatib, Laila Heilat, Wala Qudah, Salem Alhatamleh and Asef Al-Khateeb, "A novel improved deep learning model based on Bi-LSTM algorithm for intrusion detection in WSN", Network and heterogeneous Media, Volume 20, Issue 2, Pages 532–565. DOI: 10.3934/nhm.2025024

[22] Kaumudi Keerthana and A. Mahesh Babu, "A Novel Trust Management and Secure Communication Framework for Wireless Sensor Networks", Engineering, Technology & Applied Science Research, Volume 15, Issue 2, 2025, Pages 21728-21737. https://doi.org/10.48084/etasr.10009

[23] Seyed Salar Sefati, Seyedeh Tina Sefati, Saqib Nazir, Roya Zareh Farkhady and Serban Georgica Obreja, "Federated Reinforcement Learning with Hybrid Optimization for Secure and Reliable Data Transmission in Wireless Sensor Networks (WSNs)", Mathematics, Volume 13, Issue 19, 2025, Pages 1-37. https://doi.org/10.3390/math13193196

[24] Gajjala Savithri and N. Raghavendra Sai, "A Reliable Hybrid Framework for Anomaly Detection in Secure and Robust Wireless Sensor Networks", Engineering, Technology & Applied Science Research, Volume 15, Issue 4, 2005, Pages 25789-25797. https://doi.org/10.48084/etasr.11494

[25] Hongwei Zhang, Darshana Upadhyay, Marzia Zaman, Achin Jain, Srinivas Sampalli, "SC-MLIDS: Fusion-based Machine Learning Framework for Intrusion Detection in Wireless Sensor Networks", Ad Hoc Networks, Elsevier, Volume 175, 2025, Pages 1-18. https://doi.org/10.1016/j.adhoc.2025.103871

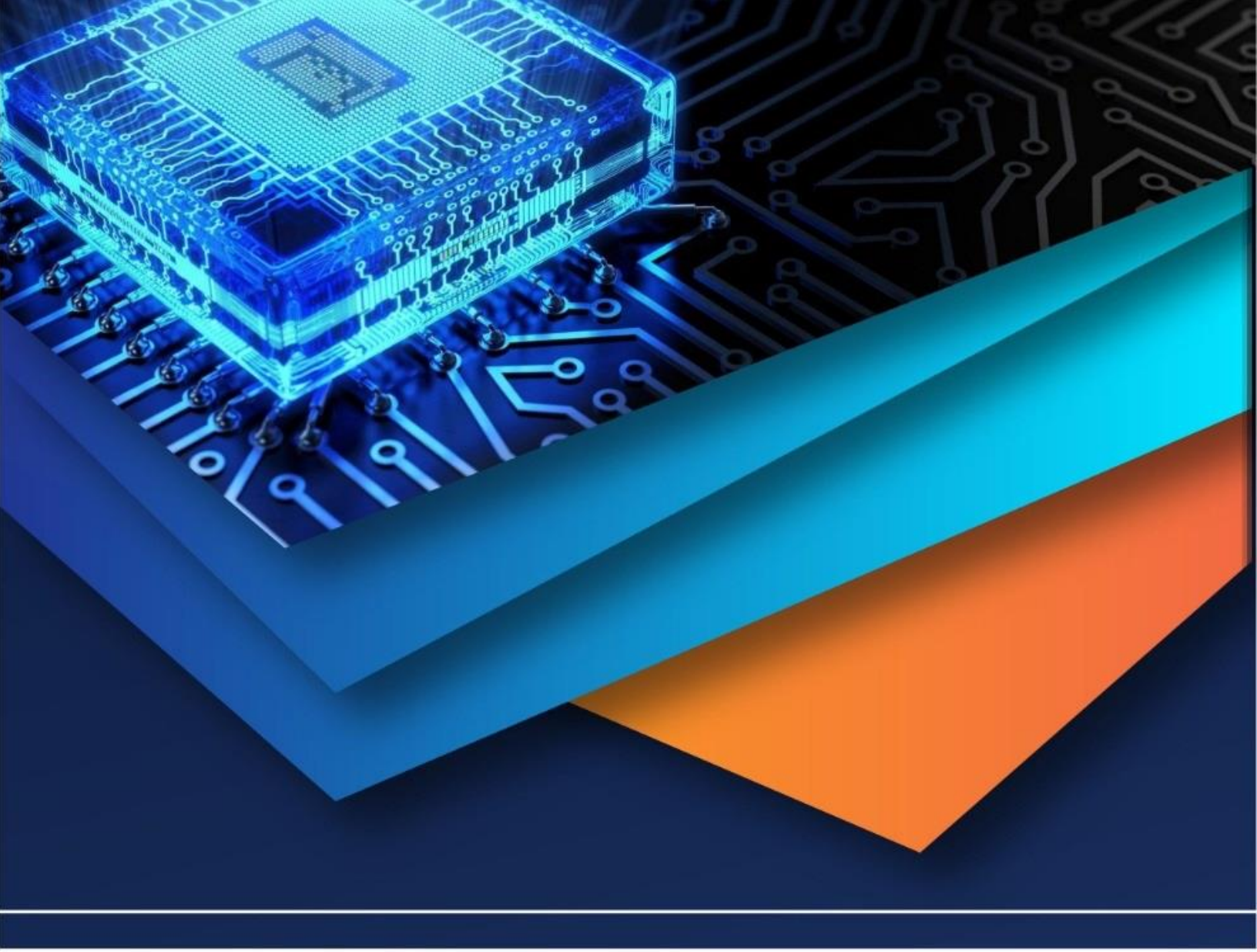
[26] Anshika Sharma and Shalli Rani, "An Optimized Ensemble Approach for Securing Wireless Sensor Networks Against Attacks", ICCK Transactions on Wireless Networks, Volume 1, Issue 1, 2025, Pages 5-15. DOI: 10.62762/TWN.2025.109626

[27] Waqar Khan, Muhammad Usama, Muhammad Shahbaz Khan, Oumaima Saidani, Hussam Al Hamadi, Noha Alnazzawi, Mohammed S. Alshehri and Jawad Ahmad, "Enhancing security in 6G-enabled wireless sensor networks for smart cities: a multi-deep learning intrusion detection approach", Frontiers in Sustainable Cities, Volume 7, 2025, Pages 1-19. https://doi.org/10.3389/frsc.2025.1580006

[28] Rahul Mahajan, Srikant V. Sonekar, "Design of an Intelligent Model for Wireless Data Security Using Graph Neural Cryptonets and Evolutionary Protocol Synthesis", International Journal of Environmental Sciences, Volume 11, Issue 3s, 2025, Pages 458-467. http://theaspd.com/index.php/ijes/article/view/308

[29] Venkatesh Prasad B.S and Roopashree H.R., "Energy aware and secure routing for hierarchical cluster through trust evaluation", Measurement: Sensors, Elsevier, Volume 33, June 2024, Pages 1-18. https://doi.org/10.1016/j.measen.2024.101132

[30] Ali Adnan Al-Khazraji, Fatimah Abdulridha Rashid, "SafeTrack: Secure Tracking Protocol for Mobile Sensor Nodes in Unstable Wireless Sensor Networks", IEEE Access, Volume 13, 2025, Pages 113736 – 113751. **DOI:** 10.1109/ACCESS.2025.3584869



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)