**Efficient Attack Detection in WSN Using Long-Short Term Memory and Convolutional Neural Networks**

**Abstract**

Wireless Sensor Networks (WSNs) are used in smart infrastructure and industrial automation. The order to monitor and send data, a WSN is made up of lots of little, limited resources sensor nodes that connect wirelessly. However, due to their limited resources and susceptibility to data injection attacks (DIA), they confront significant security challenges. Traditional attack detection methods usually suffer from high rates of false warnings, poor adaptability to new threats, and high computational costs. This paper proposed an Artificial Intelligence (AI)-based attack detection framework to improve network security and detection accuracy in WSN. The proposed method includes three key techniques: C-score normalization for static data preprocessing and normalization the raw data then next Deep Q-Learning (DQL) for dynamic and adaptive feature selection, and for detect the attacks with accurate a Long-Short Term Memory-Convolutional Neural Network (LSTM-CNN) was proposed. According to simulation results, the suggested framework enhances network security while lowering computing complexity and achieving 95.4% attack detection accuracy. This confirms the efficacy of an integrated AI-based strategy for protecting WSNs and improves the network's capacity to identify sophisticated data injection assaults.

**Keywords:** WSN, attack, transmit data, AI, C-Score normalization, network security, DQL, LSTM-CNN.

**1 Introduction**

A WSN consists of multiple sensor nodes that gather information and send it to a centre station for processing. WSNs are networks of small, low-power, dispersed sensor nodes that monitor and collect data from their surroundings. The Information is sent wirelessly to a central point for processing and examination. WSN security is critical due to the sensitive data collected and the sensor nodes' limited resources because of their wireless connection and minimal processing capability [1]. Ensuring the security of these networks is critical to various types of attacks, including DIA), which can compromise data integrity and network performance. However, the resource-constrained nature of sensor nodes, coupled with the open and dynamic network environment, makes WSNs highly susceptible to security threats such as data injection and denial-of-service (DoS) attacks [2].

These attacks can degrade network performance, compromise data integrity, and lead to significant operational disruptions. A secure solution for routing in WSNs, using a point-to-point, multi-level approach. This means that the proposed method routes data through multiple peer nodes to ensure secure and reliable communication. proposes a robust and energy-efficient solution for routing optimization in WSNs. However, the potential overhead with multi-hop routing can increase latency and energy consumption [3]. Medium Access Control (MAC) protocols for managing communication in Industrial wireless sensor networks (IWSNs), which implies that the solution involves designing or improving MAC layer protocols for better security and efficiency. The proposes improvements in MAC protocols to enhance communication efficiency and reliability. The not contain specific technical details about security paradigms and MAC protocols [4]. The development of Intrusion Detection System (IDS) for DoS attacks in WSNs. However, as the complexity and frequency of current assaults have increased, traditional IDS solutions have grown less effective [5].

The main contribute of paper is LSTM-enabled CNNs combine the advantages of LSTM-CNNs to effectively capture temporal (sequential) and spatial (structural) patterns in data. The proposed system detects anomalies in real time using an LSTM-enabled CNN model that analyses network traffic characteristics such as sensor node activity, transmission rate, signal strength, and packet order. The system combines DQL for dynamic feature selection to ensure the model focuses on the most critical network features, improves detection accuracy, and reduces false positives. This novel model allows the system to learn dynamic attack strategies and adjust to new dangers in real time. The LSTM-CNN model learns temporal patterns in network traffic through LSTM and spatial dependencies through CNN to effectively identify DIA.

**2. Literature Survey**

The context of WSNs, efficient and secure data transmission is critical for maintaining network integrity and performance. WSN nodes are designed to operate with low power consumption due to their resource-constrained nature, but the increasing complexity of modern attack detection mechanisms, such as deep learning models, introduces computational overhead. The paper presents a solid framework using Performance Indicators (PIs) and Sum of Squares (SOS) to improve the precision and stability of anomaly identification in microgrid WSNs. However, the trade-off between accuracy and computational cost and real-world scalability could be explored further [6]. In both static and dynamic distributed WSNs, replica nodes are intended to be detected and stopped by the proposed Strategic Security System (SSS). This integrates two essential techniques: SSRWND (Single-Stage Memory Random Walk with Network Division). Although the suggested approach performs better, it has several drawbacks. The system's complexity may increase computational load, affecting real-time performance and energy efficiency [7].

The security challenges facing UWSNs. They provide a detailed taxonomy of UWSNs based on from research databases. Despite thoroughly analysing UWSN security challenges, the paper does not propose a concrete solution or a new security framework [8]. The Online Locally Weighted Projection Regression (OLWPR) model for WSN anomaly detection. OLWPR is a non-parametric method in which current predictions are made using local functions based on a small portion of data, reducing computing complexity—an important requirement for WSNs with limited resources. While the suggested OLWPR model produces promising results, that does have significant drawbacks. First, the detection rate of 86% has space for improvement, particularly in mission-critical applications requiring more accuracy [9]. This algorithm called M-Path Sinkhole Attack Detection (MSAD). MSAD is designed to work with resource-constrained WSN devices such as sensor nodes. The algorithm uses a clustering-based approach to reduce energy consumption and extend the network lifetime. Although MSAD exhibits high detection accuracy, this also has some limitations. First, this paper does not address the potential impact of the network lifetime and the impact of the increased communication overhead due to clustering on performance [10].

The optimized deep neural network (DNN) technique for threats detection. The key parameters of the DNN are set using the Adaptive Particle Swarm Optimization (APSO) approach to improve precision of detection and decrease of false positives. This method detects and mitigates DoS attacks using network behaviour and transmission patterns. The proposed approach improves detection accuracy and network performance but has some limitations [11]. The novel framework called GAN-based Clustering and LSTM-based Data Aggregation (GCLD) to enhance the Quality of Service (QoS) in WSNs and reduce communication delay due to improved clustering and data aggregation. However, GAN and LSTM models require high computational power, which may strain the limited resources of sensor nodes [12].

The Stacked Convolutional Neural Network and Bidirectional (SCNN-Bi-LSTM) model integrated for intrusion detection in WSNs. However, SCNN, and Bi-LSTM models require more memory and processing power, which may strain the limited resources of WSN nodes [13]. The next step is to use particle swarm optimization (PSO) to select features. Compared with previous intrusion detection methods, the proposed framework outperforms them. However, the combination of PSO, CNN, and Bi-LSTM increases processing requirements and may burden the limited resources of WSN nodes [14].

The IDS based on Gated Capsule Networks (GCN). The proposed method combines two advanced techniques: the Spotted Hyena Optimizer (SHO). The GCN is intended to increase the precision of identifying anomalous activity in WSN. Despite its high performance, the proposed framework has certain limitations. The combination of GCN, SHO, and GRU increases the computational complexity, which may pose challenges for low-power devices in large-scale deployments [15].

The IDS that combine the characteristics of CNN and STM networks. The model can identify complex trends in network traffic data thanks to CNN's application for spatial feature extraction. The proposed CNN-LSTM model produced excellent detection rates, significant accuracy, and a low error rate. However, using CNN and LSTM increases the model complexity, which leads to high computing costs and long training times [16]. A Q-learning-based information exchange routing technique to optimize energy consumption and extend the future of WSN. The adaptive feature of Q-learning enables the network to respond to changing conditions while maintaining energy efficiency over time. Despite advantages, the proposed approach introduces computational complexity due to the Q-value optimization process, which may increase latency [17].

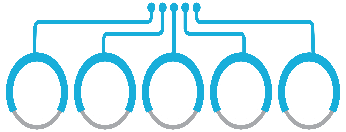
They introduce an RL-based routing strategy for Software-defined Wireless sensor networking SDWSNs to enhance power efficiency and QoS. Despite advantages, the RL-based approach introduces additional computational complexity due to the learning process, which may increase processing time and resource consumption [18]. And a (DQL) Energy-Optimized LoS/NLoS (DQLEL) architecture for improving UWB-based indoor localization. However, due to the complexity of the DQLEL framework introduces high computational overhead [19]. CNNs are employed to derive spatial patterns from network traffic data, while Bi-LSTMs are utilized to learn past and future temporal relationships in the data, making the model better able to identify dynamic and complex patterns. Nonetheless, the model is likely to be computationally complex, not scalable, and lacks real-world verification [20].

**3. Proposed Methodology**

The LSTM-CNN handles attack detection, while C-Score Normalization improves data consistency during preprocessing, making learning more efficient and decisions more reliable. DQL selects the most important features to improve detection accuracy and reduce processing load in WSNs.

C-Score Normalization

Data set



Mean

Standard Deviation

Normalized Data

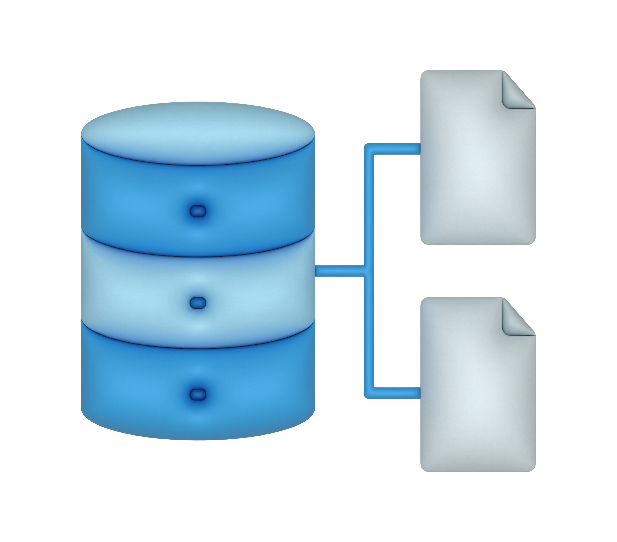
Define State

Select Action

Optimized Feature Set

Deep Q-Learning

Attack Detection → LSTM-CNN



CNN (Spatial Extraction)

LSTM (Temporal Dependency)

**Output Classification**

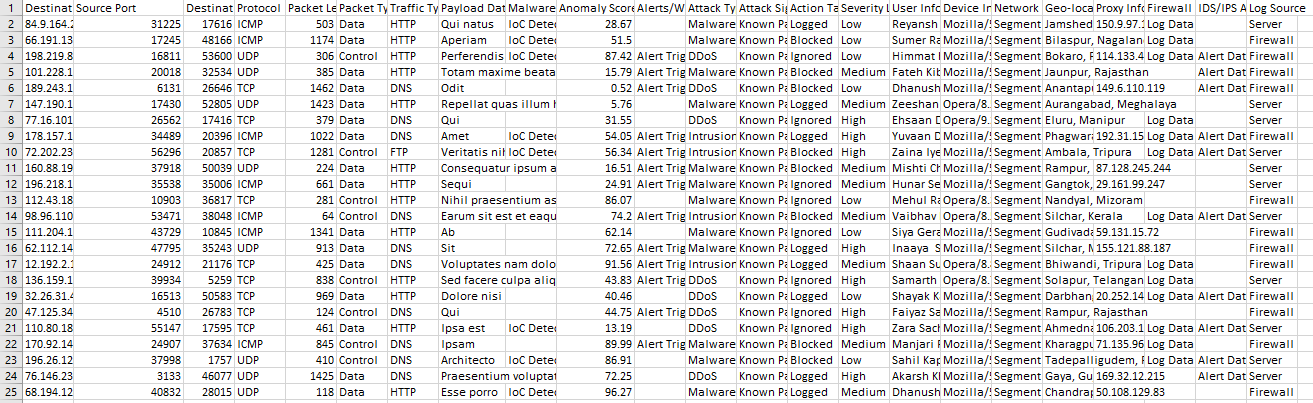


input

**Figure 1: Architecture diagram illustrating the suggested approach**

The figure 1 shows the data flow through a WSN using C-score normalization for preprocessing, DQL for feature selection, and LSTM-CNN for attack detection and classification. Sensor nodes collect and transmit data. The data is processed using C-score normalization, first calculating the means and standard deviations to ensure normalization for standard learning. The normalized data is fed into a DQL module. DQL defines the current state of the network based on the input data, selects the best actions to improve the relevance of the features, and outputs the most important features for attack detection. This helps the adaptive feature selection model focus on the most informative signals, improving detection performance. The LSTM-CNN model processes the selected features. The LSTM layer captures the temporal dependence in the data and identifies patterns over time. On the other hand, CNN layers extract spatial features and identify structural patterns in the data. The combined output is used to classify normal or malicious data, effectively detect data DIA, and prevent network outages.

This Data set is gathered from the Kaggle website: <https://www.kaggle.com/datasets/teamincribo/cyber-security-attacks/versions/7/data> . This data set contains more than 40000 Cyber Attack data values.



This Figure 2 presents the Cyber Attack Data set that contains the 40,000 malware attack values, and every data value and protocol and Anomaly Scores and more of the Cyber-threats attack information.

**3.2 C-Score Normalization**

This section C -Score Normalization work is reducing the null and noise data from the raw data set, compared to another traditional method. The C-Score Normalization is to minimize the null valid information from the data collection. The data is processed using C-score normalization, first calculating the means and standard deviations to ensure normalization for standard learning. To Normalize sensor data collected from WSNs to a standard scale, and improves the stability of the training process in the DQL and LSTM-CNN models by reducing variations in input data. A statistical metric known as the C-Score shows, in terms of standard deviation, how far a given data point deviates from the dataset mean.

Equation 1 where is the C-Score of the data point, is the value of the data, σ is the standard deviation of the data, μ is the mean of the data.

(1)

The process begins with the collection of raw sensor data from the WSN nodes. First, the mean of the input data is calculated using this equation 2.

(2)

where N represents all of the data points. After that, the standard deviation is computed using equation 3.

(3)

Following the mean and standard deviation calculation, the C-Score is applied to every data point to adjust. This will stretch the data concerning overall distribution to improve the detection of patterns and anomalies. The scaled data is now passed through to the DQL model to extract the most beneficial features. This enables the model to concentrate on essential tasks that enhance network security and identify attempts at data breaches.

**3.2 Deep Q-Learning (DQL)**

DQL is an RL method that solves challenging decision-making problems by fusing deep neural networks with the ideas of Q-L. To increase the precision and effectiveness of attack detection models in WSNs, the most pertinent elements from sensor data must be chosen. By allowing the model to dynamically choose the most informative characteristics, DQL lowers noise and enhances detection capabilities.

With the help of the value-based training algorithm Q-Learning, an agent can learn to act optimally in a certain state by considering the anticipated future reward. In DQL, the Q-value function—which denotes the expected reward of performing a specific action in a specific state—is approximated using a deep neural network. Equation 4 is utilised to update the Q-value.

(4)

Equation 4 where is the -value for the current state s and action , is the learning rate that controls how quickly the model updates the knowledge, is the reward received after taking action , is the discount factor that determines the importance of future rewards, is the next state after taking action , and is the next possible action.

After selecting a feature, the model receives a reward based on how informative and relevant the selected feature is for attack detection. The reward function is defined as:

(5)

Equation 5 where represents the information gain from the selected feature, and is the computational cost of selecting the feature. The Q-value is then updated using the reward and the predicted Q-value for the next state. A deep neural network is used to approximate the Q-values, and its weights are adjusted using backpropagation based on the loss function.

(6)

Equation 6, Where stands for the network settings, the model keeps improving the decision-making by reducing errors and better estimating the Q-value. This repeated learning process, the DQL model slowly learns to focus on the most important features, ignoring unnecessary data and simplifying the input. The selected features are then passed to the attack detection LSTM-CNN for classification. DQL enhances efficiency in general of the attack monitoring system by selecting the most valuable features and continuously adapting to the changing network conditions.

**3.3 Long-Short Term Memory-Convolutional Neural Network (LSTM-CNN)**

The LSTM-CNN model is a deep learning technology that combines of CNN and LSTM networks to improve the accuracy of attack detection in WSNs. Sensor data in WSNs frequently exhibits both spatial and temporal interdependence, which must be efficiently recorded in order to detect anomalies with accuracy. The LSTM-CNN model employs both LSTM's ongoing learning capability and CNN's feature extraction skills to more accurately detect DIA.

The process begins with input data collected from WSN nodes. After undergoing preprocessing and feature selection using DQL. The input data consists of time-series data, which includes parameters such as node status, transmission rates, and network traffic patterns. The LSTM layer is the model's initial step. In contrast to conventional RNNs, which have issues with vanishing gradients, LSTM retains long-term memory by controlling the input flow through the network through a gating mechanism. The three main gates that make up each LSTM unit are the input, output, and forget gates. The quantity of data that is saved, updated, and sent to these gates control the subsequent time step.

The Forget Gate governs how much of the prior memory (cell state) is preserved or lost. This enables the model to "forget" irrelevant data while maintaining relevant patterns. The Forget Gate value at time step is calculated using the sigmoid formula. The sigmoid equation 7, produces values between 0 and 1. If the value is close to zero, most of the prior information is lost, whereas a value close to one maintains the majority of the previous memory.

(7)

The Input Gate controls how much new information from the current input should be added to the cell state. This regulates the impact of the new input on the network's memory. The Input Gate value is = input gate output at time computed using equation 8.

(8)

(9)

Equation 9, where ​ = candidate cell state. ​ = matrix of weights for the potential state. = bias term in addition, a candidate cell state is computed using the hyperbolic tangent (tanh) function activation to control the amount of newly added memory.

The cell state equation 10 represents the memory of the LSTM. It is updated based on the forget gate and input gate values. The updated cell state at time step is computed as. The cell state allows the model to carry long-term information across multiple time steps, preserving important sequential patterns that are essential for detecting anomalies in network traffic.

(10)

The Output Gate controls how much of the cell state may be transferred to the concealed state and propagate to the next layer. The acts as a filter that allows only the most relevant information to pass through. The Output Gate value is computed the equation 11.

(11)

The CNN layer applies convolutional filters to the hidden state to extract spatial correlations and patterns. The convolution operation is defined as equation 12.

(12)

The CNN layer applies convolutional filters to the hidden state to extract spatial correlations and patterns. where, ​ = CNN output at position for the kth filter. = convolutional kernel weights. = bias. = activation function (e.g., ReLU). The convolution operation is defined as equation 12.

The output from the CNN layer is passed through a gating mechanism that regulates the amount of information passed to the next stage. The gate value is computed as equation 13. The gated output is passed to a dense layer, where a SoftMax classifier predicts whether the input data represents normal or malicious traffic. The final output represents the attack detection result.

(13)

The proposed method is a strong and effective way to protect WSNs from data DIA. By combining data preprocessing, and advanced deep learning models, the system achieves high detection accuracy while keeping processing costs low. The LSTM-CNN model identifies both short-term and long-term patterns, offering reliable protection against new cyber threats in WSNs.

**4. Results and Discussion**

This part describes the analysis and outcomes of the simulation associated with implementing AI-driven attack Detection in the WSN systems considering security and detection precision enhancements. The system metrics comprise the false positive rate (FPR), detection accuracy, energy expenditure, and F1-Score. Results demonstrate how the integrated approach of C-Score Normalisation, DQL, and LSTM- CNN increases detection performance and the network's robustness against Distributed Intelligent attacks (DIA). The model shows better accuracy, fast convergence, and adaptability to dynamic network changes, suggesting efficacy in dynamic real-time attack detection and avoidance.

**Table 1: Simulation Setup for NS-2**

|  |  |
| --- | --- |
| **Parameter** | **Value** |
| **Simulation Tool** | Python |
| **Data set** | Cyber Security Attacks |
| **Number of Nodes** | 40000 |
| **Packet Size** | 513 bytes |
| **Node Speed** | 1–25 m/s |
| **Energy Model** | 100 Joules (initial energy) |
| **Traffic Type** | Constant Bit Rate (CBR) |

Table 1 shows the model setup used to evaluate the proposed framework for enhancing attack detection and network performance in WSN. The NS-2 simulator is employed because this can effectively model and analyse WSN environments. The network topology consists of 100 sensor nodes deployed within a 1000 m × 1000 m area, simulating a realistic network environment.

**Figure 2. Detection Accuracy**

Figure 2 shows analogy of the detection precision of the suggested LSTM-CNN approach with two existing approaches: SVM-based detection and OLWPR. The LSTM-CNN model achieved approximately 90% to 100% accuracy, significantly outperforming SVM (which reached 30% to 50%) and OLWPR (which reached 40% to 80%) under different network conditions. This demonstrates that the LSTM- CNN model effectively identifies malicious activity in WSNs. This strong performance stems from its ability to record spatial and patterns of time in the data, allowing for accurate detection of abnormal traffic and data DIA.

**Figure 3. False Positive Rate**

Figure 3 shows the FPR analysis for the LSTM-CNN method compared to earlier methods like SVM-based detection and OLWPR. The new method significantly lowers the FPR, reaching around 5% to 15% in different situations, which is much better than SVM (30%–50%) and SOS (20%–40%). This improvement is because the LSTM-CNN can better recognize and separate normal and malicious patterns, making the system more accurate and reliable at detecting DIA in WSNs.

**Figure 4. Energy Efficiency**

Figure 4 shows the energy consumption of the proposed LSTM- CNN method compared to other approaches, including SVM-based detection and SOS-based clustering. The LSTM-CNN framework consumes approximately 20% to 40% less energy under different node configurations, significantly lower than SVM (55% to 70%) and OLWPR (40% to 60%). Reduced energy consumption extends the network's lifespan and enhances performance in WSNs.

**Figure 5. F1-Score**

Figure 5 illustrates the F1-Score performance of the suggested LSTM-CNN approach in contrast to other approaches, including OLWPR-based detection and SVM-based classification. The LSTM- CNN framework achieves an F1-Score of approximately 75% to 90% under various node configurations, outperforming SVM (60% to 75%) and OLWPR (40% to 55%) enhances performance in WSNs.

**5. Conclusion**

The proposed new security methodology for WSNs intends to control Denial of Service attacks by implementing three major techniques of pre-processing the dimensionality of data by using C-Score Normalization, feature selection using DQL, and finally using LSTM-CNN for anomaly detection. The LSTM-CNN approach extracts patterns of harmful data and timestamps associated with them to be able to identify the basic patterns of the data. With the removal of redundant features, the DQL aids in improving the accuracy of detection, while the C-Score Normalization assists in improving the power of the model by providing the data with uniform scaling. The results indicate this model can detect attacks with 95% accuracy, provides a PDR of 92%, and reduces the false alerts is received. Besides, this countermeasure provides a reduction of energy consumption by 14% compared to previous approaches, leading to an increase in the lifetime of the networks. The tremendous enhancement of WSN security and performance due to a combination of anomaly detection using LSTM, selection of features using DQL, and data pre-processing according to C-Score Normalization is unquestionable.

**Reference**

1. Ahmad, Rami, Raniyah Wazirali, and Tarik Abu-Ain. "Machine learning for wireless sensor networks security: An overview of challenges and issues." Sensors 22.13 (2022): 4730.
2. Huanan, Zhang, Xing Suping, and Wang Jiannan. "Security and application of wireless sensor network." Procedia Computer Science 183 (2021): 486-492.
3. Olakanmi, Oladayo Olufemi, and Adedamola Dada. "Wireless sensor networks (WSNs): Security and privacy issues and solutions." Wireless mesh networks-security, architectures and protocols. IntechOpen, 2020.
4. Bhushan, Bharat, and Gadadhar Sahoo. "Requirements, protocols, and security challenges in wireless sensor networks: An industrial perspective." Handbook of computer networks and cyber security: principles and paradigms (2020): 683-713.
5. Salmi, Salim, and Lahcen Oughdir. "Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network." Journal of Big Data 10.1 (2023): 17.
6. Kavousi-Fard, Abdollah, Wencong Su, and Tao Jin. "A machine-learning-based cyber-attack detection model for wireless sensor networks in microgrids." IEEE Transactions on Industrial Informatics 17.1 (2020): 650-658.
7. Sujihelen, L., et al. "Node replication attack detection in distributed wireless sensor networks." Wireless Communications and Mobile Computing 2022.1 (2022): 7252791.
8. Ahmad, Irfan, et al. "Analysis of security attacks and taxonomy in underwater wireless sensor networks." Wireless Communications and Mobile Computing 2021.1 (2021): 1444024.
9. Poornima, I. Gethzi Ahila, and B. Paramasivan. "Anomaly detection in wireless sensor network using machine learning algorithm." Computer communications 151 (2020): 331-337.
10. Shanmugaraja, P., et al. "An Efficient Clustered M-path Sinkhole Attack Detection (MSAD) Algorithm for Wireless Sensor Networks." Adhoc & Sensor Wireless Networks 55 (2023).
11. Shanmugaraja, P., et al. "An Efficient Clustered M-path Sinkhole Attack Detection (MSAD) Algorithm for Wireless Sensor Networks." Adhoc & Sensor Wireless Networks 55 (2023).
12. Hemalatha, K., and M. Amanullah. "Effective Hybrid Deep Learning Model of GAN and LSTM for Clustering and Data Aggregation in Wireless Sensor Networks." International Journal of Sensors Wireless Communications and Control 14.2 (2024): 122-133.
13. Bukhari, Syed Muhammad Salman, et al. "Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability." Ad Hoc Networks 155 (2024): 103407.
14. ARUMUGASAMY, S. "An Intrusion Detection Approach In Wireless Sensor Network Security Through CnnBi-Lstm Model." Journal of Theoretical and Applied Information Technology 102.2 (2024).
15. Arivazhagu, U. V., et al. "Gated Capsule Networks for Intrusion Detection Systems to Improve the Security of WSN-IoT." Adhoc & Sensor Wireless Networks 56 (2023).
16. Halbouni, Asmaa, et al. "CNN-LSTM: hybrid deep neural network for network intrusion detection system." *IEEE Access* 10 (2022): 99837-99849.
17. Su, Xing, et al. "A Q-learning-based routing approach for energy efficient information transmission in wireless sensor network." *IEEE Transactions on Network and Service Management* 20.2 (2022): 1949-1961.
18. Younus, Muhammad Usman, Muhammad Khurram Khan, and Abdul Rauf Bhatti. "Improving the software-defined wireless sensor networks routing performance using reinforcement learning." *IEEE Internet of Things Journal* 9.5 (2021): 3495-3508.
19. Hajiakhondi-Meybodi, Zohreh, et al. "DQLEL: Deep Q-learning for energy-optimized LoS/NLoS UWB node selection." *IEEE Transactions on Signal Processing* 70 (2022): 2532-2547.
20. Bukhari, Syed Muhammad Salman, et al. "Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability." *Ad Hoc Networks* 155 (2024): 103407.