Secure Knowledge and Cluster based Intrusion Detection Mechanism for Smart Wireless Sensor Network

Devi. D[1], Hemalatha S[2], Kaviyapriya R[3], Malaiyammal T[4], Abinaya S[5]
[1]*Assistant Professor, Department of Computer Science and Engineering, Maha Barathi Engineering College (Affiliated to Anna University), Chinnasalem (Tk), Kallakurichi (Dt)-606 201.*
[2,3,4,5]*UG Student, Department of Computer Science and Engineering, Maha Barathi Engineering College (Affiliated to Anna University), Chinnasalem (Tk), Kallakurichi (Dt)-606 201.*

***Abstract*—Wireless Sensor Networks (WSNs) are deployed frequently across applications, including environmental monitoring, military surveillance, and health care systems. The constrained resources and open network channels in WSNs require robust IDS development because they create exposed security threats. WSN security relies heavily on IDS systems that detect harmful network events to protect network reliability and integrity. Trusted Intrusion Detection Systems operate with weak attack identifications, elevated system power usage, and restricted capabilities when detecting changing attack types. This paper introduces a secure knowledge and cluster-based Intrusion Detection System that combines Artificial Bee Colony-Long Short-Term Memory (ABC-LSTM) methodology to solve existing challenges. The outlined strategy is comprised of three fundamental steps; the first step is the formation of clusters utilizing the Low-Energy Adaptive Clustering Hierarchy (LEACH) method, which utilizes cluster forming to improve the energy consumption and scalability of the network; then follows feature selection with the Ant Colony Optimization (ACO) algorithm, which selects the most suitable cluster features intending to attain the highest detection accuracy with the lowest possible computational burden; and finally, intrusion detection ABC-LSTM, wherein hyperparameters of LSTM networks are tuned with the Artificial Bee Colony (ABC) method to enhance the efficiency of anomaly detection. The proposed method provides WSNs with adaptive intrusion detection systems that deliver energy efficiency with high accuracy. Simulation outcomes show that our solution delivers better IDS performance than standard IDS systems regarding detection capabilities, energy efficiency, and false alarm reduction, establishing it as an effective defensive measure for WSN security.**

***Index Terms*—WSN, IDS, threats, malicious activities, cluster, LEACH, ACO, ABC-LSTM, anomaly detection**

I. INTRODUCTION

The WSN, with smart capabilities, is a modern communication network that uses distributed sensors to monitor environmental conditions while transmitting their findings across space. Wireless Sensor Networks have applications across numerous fields, such as industrial control systems, healthcare and military observations, and environmental measuring systems. Security threats from intrusion attacks threaten smart Wireless Sensor Networks because these networks operate with limited resources across many distributed nodes through unsecured communication paths. System failures and inaccurate decision-making occur because unauthorized access, malicious node injection, and denial-of-service attacks impact data integrity. Building smart WSN security is a vital operational challenge that requires smart and effective intrusion detection systems [1].

IDS operates within WSN networks to provide security through detection systems that defend against malicious activities in the network. According to [2], IDS consists of two detection categories: anomaly-based and signature-based systems. Signature-based IDS operates using pre-established attack signatures, which generates high efficiency for recognized attacks while showing an inability to handle new security threats [3]. Anomaly-based IDS utilizes machine learning and Artificial Intelligence (AI) to find changes in typical network activities, which helps detect unknown security threats. WSN IDS operates through a typical workflow, which starts from data collection, proceeds to feature extraction, moves to attack detection, and ends with response mechanisms. The analysis through machine learning algorithms enables sensor nodes to process network data into

normal or malicious classifications from continuous monitoring activities. After detecting an intrusion, the security system deploys the required countermeasures to defend the network against potential threats.

The current IDS solutions used in WSNs encounter multiple serious obstacles. The main weakness of anomaly-based detection involves high incorrect alarm rates because normal traffic variations get mistaken for attacks [3]. The limited power availability in WSNs makes it problematic to install sophisticated detection approaches because their resource demands shorten the network's lifetime [4]. Traditional IDS systems face scalability problems while implementing vast networks that experience shifting topology structures [5]. Many IDS solutions today lack effectiveness when dealing with modern adversary threats like zero-day attacks and adversarial ML attacks that break through traditional security defenses. Stronger and more cognitive IDS frameworks require development to strengthen their detection abilities without compromising their energy consumption levels.

II. LITERATURE SURVEY

Several research studies and academic publications have focused on Wireless Sensor Network (WSN) intrusion detection because they introduce ML and DL strategies to improve security while enhancing detection performance. The authors in [6] demonstrated an ML-based IDS that used state-of-the-art classification methods but experienced high computational processing burdens, leading to real-time implementation hurdles. The Deep Neural Network (DNN)-based IDS proposed in [7] generated better efficiency results during intrusion detection yet required large training data, which led to architectural overfitting issues.

Implementing an optimized DL-based IDS from [8] failed to maintain effective security adaptations because it lacked suitable mechanisms to adapt to dynamic WSN environments. The authors in [9] combined security protection with energy efficiency in their DL-based routing mechanism through IDS integration, but the advanced model features created time delays for real-time deployments.

The author [10] demonstrated an optimization-enhanced DL-based IDS with dual trust assessment layers that created highly reliable detections but required cumbersome data handling processes to implement. The authors in [11] developed a DL IDS that used a wrapper-based feature extraction method but experienced processing delays because feature extraction mechanisms are resource-intensive.

A real-time IDS built with DL in [12] gained speed and accuracy advantages, yet its performance decreased when facing unknown threats because it was based on predefined patterns. The MLSTL-WSN model implemented SMOTETomek preprocessing for addressing data imbalance yet required extended training durations because of this additional step, according to [13]. A network security system presented in [14] used Whale Optimization Algorithm-Artificial Bee Colony (WOA-ABC) combined with Convolutional Neural Network (CNN) but needed excessive computing power, which restricted its usage in resource-restricted WSNs.

The IDS system proposed in [15] depended on CNNs to boost its classification capabilities, yet it could not adapt to new threats, which demanded recurrent training for effectiveness.

III. PROPOSED METHODOLOGY

This section briefly describes the cluster-based IDS method for secure smart WSN. To secure the smart WSN, the proposed method performs three phases: cluster creation, selecting the features of clusters, then finding the attack or normal in the network cluster. The LEACH method is used for cluster creation, ACO is used to select the appropriate features in deploy clusters, and the ABC-LSTM-based IDS is used to classify normal or attack accurately.

In figure 1 we illustrate the architecture diagram of the deployed method. The network uses the LEACH method to arrange sensor nodes into clusters for efficient energy management and prolonged operation time. Clusters select their Cluster Head (CH) to aggregate data and forward it to the base station, thus minimizing redundant transmission. Feature selection through ACO identifies crucial cluster features in the second phase to enhance the detection process while reducing complexity. The system keeps essential data exclusively, while all other data remains unprocessed during the intrusion detection period. The intrusion detection system relies on the ABC-LSTM model that optimizes the ABC algorithm to enhance LSTM hyperparameter values for improved anomaly

detection effectiveness. The trained model defines network action as normal or harmful to establish an adaptive security framework for WSNs.

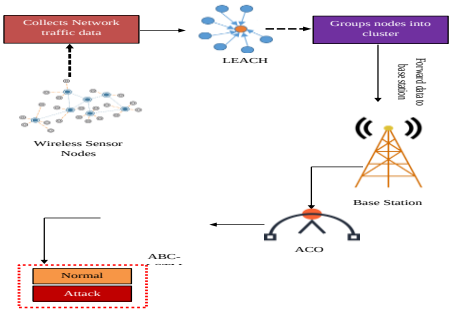

Fig. 1 Architecture Diagram of the proposed method

A. Low-Energy Adaptive Clustering Hierarchy (LEACH)

Low-Energy Adaptive Clustering Hierarchy (LEACH) is a hierarchical routing protocol that uses cluster formation to control energy expenditures inside WSN. The system has a policy for rotating Cluster Head (CH) selection between nodes to achieve balanced energy consumption across the network. The CH operates as the central processor that gathers data from its cluster members, then sends the evaluated information to the base station, improving efficiency and network life span. Combining regularly rotating Cluster Heads with data aggregation allows LEACH to reduce power consumption, improving network performance and operation duration.

$$P(i) = \begin{cases} \frac{p}{1-p\times\left(r \bmod \frac{1}{p}\right)}, & if\ i \in G \\ 0, & otherwise \end{cases} \quad (1)$$

Each round of LEACH runs a threshold function, which sensor nodes use to determine CH selection using a predefined probability value P. Nodes that have not recently served as cluster heads have higher selection probabilities to achieve better energy distribution. The equation enables CH responsibility to spread evenly among sensors throughout time, protecting nodes from premature exhaustion.

$$E_{CH} = mE_{recv} + E_{agg} + E_{trans}(d) \quad (2)$$

Equation 2 comprises E_{CH} as the energy consumed by the cluster head and m as the number of member nodes in the cluster, along with E_{recv}, which is the energy needed to receive data from each member node, and E_{agg}, representing the energy required for data aggregation and transmission energy $E_{trans}(d)$ for distance d and after selection as the CH node becomes responsible for collecting data from member nodes, then reducing data redundancy before sending processed information to the base station. The CH energy utilization relates to receiving data and aggregating it, followed by sending it to a base station over a particular range. The equation guarantees that the decision node selects data processing methods that maintain high operational effectiveness while staying within their power capacity.

$$E_{node} = E_{trans}(d_{CH}) \quad (3)$$

The main power usage of member nodes in a cluster occurs when they transmit their measurement data to their designated CHs. Overall energy consumption decreases when CHs are placed where the transmission energy remains minimal between the member nodes and CHs. The equation shows that the member node transmission energy needs decrease when the optimal Cluster Heads position themselves correctly.

$$E_{trans}(d) = \begin{cases} LE_{elec} + L_{\in f_s} d^2, & d < d_0 \\ LE_{elec} + L_{\in mp} d^4, & d \geq d_0 \end{cases} \quad (4)$$

This equation represents the energy calculation for data transmission, where L stands for transmitted bits and E_{elec} indicates circuit operation energy consumption, and the two amplification factors $\in f_s$ and $\in mp$ are linked with free-space and multi-path models, while d_0 indicates their distance threshold. Data transmission energy consumption depends on the distance between the sender and the receiver, and the transmission energy model evaluates this energy level. The transmission follows a free-space propagation model when distances are brief and requires energy based on d^2. When a fusion of free-space propagation model and multi-path fading model operates for extended ranges, it requires energy at a rate of d^4. Network optimization results from this equation because it reduces energy loss during data transmission.

$$E_{round} = k(E_{CH} + mE_{node}) \quad (5)$$

where, k is the number of clusters. One round of LEACH-based protocol operation requires network nodes and CH to use energy across all clusters. The LEACH approach maximizes WSN life span by rolling cluster numbers and optimizing CH selection to achieve balanced energy consumption levels. The equation enables efficient protocol evaluation, aiding in developing improved clustering methods.

B. Ant Colony Optimization (ACO)

Ant Colony Optimization (ACO) performs feature selection in the second detection process phase, which identifies essential cluster features to achieve better accuracy while simplifying computations. Detailing ant foraging behavior enables ACO to assess candidate feature subsets and choose those exhibiting maximum relevant characteristics through probabilistic evaluation. The method allows the system to conserve fundamental data for processing by removing unneeded or duplicate information. The analysis point during intrusion detection solely relies on selected features to enhance performance while consuming limited resources without affecting detection capability.

$$P(f_i) = \frac{\tau_i^{\alpha}.\eta_i^{\beta}}{\sum_{j \in F} \tau_i^{\alpha}.\eta_i^{\beta}} \quad (6)$$

When measuring intrusion detection relevance, the probability of selecting cluster feature f_i depends on its pheromone level τ_i, together with its heuristic value η_i. Pheromone intensity and heuristic information influence the selection process by regulating the α and β parameters. The system achieves equal probability distribution among cluster features through the denominator, so important attributes are chosen for analysis, while less standard but still valuable features can be evaluated. The probability function is a feature optimization tool that provides accurate results and efficient detection systems.

$$\tau_i(t+1) = (1-\rho)\tau_i(t) + \sum_{k=1}^{m} \Delta\tau_i^k \quad (7)$$

During each iteration, the pheromone level τ_i for each cluster feature undergoes an update that calculates its past contribution to selection metrics. The evaporation ρ rate in the model operates to avoid excessive reinforcement of particular features and maintains selection variety. A merging of multiple pheromone contributions allows high-quality features to be frequently selected to receive intensified reinforcement from numerous ants m. The system reaches its most informative cluster features through a gradual convergence process which simultaneously keeps its system adaptable.

$$\Delta\tau_i^k = \frac{Q}{J_k} \quad (8)$$

Through equation 8, each ant uses pheromone deposition $\Delta\tau_i^k$ on the selected cluster features based on the quality of their subset. Each pheromone deposition at index i and cluster k depends on a constant value Q and the fitness measurement J_k, which rates the selected feature classification performance. The pheromone deposition process strengthens the selection mechanism for intrusion detection features, giving higher importance to relevant features in further iterations. This formula enables threat detection more effectively by establishing high-quality features precedence over others.

$$J(S) = w_1.A(S) - w_2.R(S)\, J(S) \quad (9)$$

Functions as the fitness score to assess clusters S by combining the classification accuracy A and the redundancy R reduction. The subset detection accuracy $A(S)$ defines the measurement of intrusion detection performance, but the redundancy reduction term $R(S)$ minimizes unnecessary and correlated features. The weighting factors w_1 and w_2 regulate the objectives since they balance detection efficiency and computational resource usage when selecting cluster features.

$$\max(\tau_i) - \min(\tau_i) < \epsilon \quad (10)$$

The pheromone-based clustering approach ends when the pheromone values throughout clusters reach equilibrium, with ϵ being the threshold limit. The algorithm stops working to minimize computational waste because it recognizes when it locates the best cluster feature subset. The system combines efficiency with high detection through a defined stopping criterion.

C.Artificial Bee Colony-Long Short-Term Memory (ABC-LSTM)

The IDS implements the ABC-LSTM model to optimize LSTM parameters using the ABC method between the detection process and feature selection to achieve more precise anomaly detection. The ABC algorithm replicates honeybee foraging processes to optimize three crucial LSTM parameters to attain peak performance, including learning rate, hidden layer quantity, and batch parameters. The analyzed network traffic patterns guide the trained LSTM model to classify all actions as normal operations or harmful incidents. Security in WSNs becomes stronger through this adaptive solution because it provides dynamic intrusion detection alongside automatic false alarm reduction and enhanced detection performance to build an intelligent security framework.

$$J(H) = w_1.E(H) + w_2.C(H) \quad (11)$$

The fitness function $J(H)$ assesses the quality within a specific hyperparameter set H. The

classification error term $E(H)$ employs cross-entropy loss or mean squared error to determine how precisely an LSTM model detects normal versus harmful network activity. The complexity term $C(H)$ is a computational efficiency penalty discouraging overusing hidden layers with large batch sizes. Through weighting factors w_1 and w_2, the ABC algorithm balances performance accuracy and system efficiency to optimize hyperparameters for real-time WSN IDS operation.

$$H_i^n = H_i + \emptyset.(H_i - H_j) \quad (12)$$

The algorithm of ABC determines the adjustment of H_i (current parameters) by selecting a random solution H_j from other bees. The exploration factor $\emptyset$ introduces randomness to selection, ranging from $[-1,1]$, which enables the search process to move away from stagnant points and discover many different configurations. The equation allows for the ABC algorithm to refine H_i, thus finding the best learning rates, hidden layers, and batch sizes that improve the performance of LSTM in detecting network intrusions.

$$f_t = \sigma(W_f.[h_{t-1}, x_t] + b_f) \quad (13)$$

The forget gate f_t within this equation controls the retention level of C_{t-1} through x_t and h_{t-1}. The decision output range of the sigmoid activation function σ runs between complete forgetting (value of 0) and full retention (value of 1).

$$i_t = \sigma(W_i.[h_{t-1}, x_t] + b_i)$$
$$\tilde{C}_t = \tanh(W_C.[h_{t-1}, x_t] + b_C) \quad (14)$$

The input gate i_t controls the degree of new input information admission into the cell state. Tanh applies an activation function to generate the transformed candidate state $\tilde{C}_t$ to achieve balanced updates.

$$C_t = f_t.C_{t-1} + i_t.\tilde{C}_t \quad (15)$$

The LSTM achieves memory update through an operation that blends existing information from C_{t-1} using f_t weights with new information $\tilde{C}_t$ via i_t weights. The network can focus on keeping significant network patterns through this mechanism, which simultaneously eliminates background variations.

$$o_t = \sigma(W_o.[h_{t-1}, x_t] + b_o)$$
$$h_t = o_t.\tanh(C_t) \quad (16)$$

The LSTM unit gets its definition from the output gate o_t within this equation. tanh activation transforms C_t to h_t, which results in the hidden state generation by multiplying it with o_t. The mechanism allows the system to recognize only vital information that identifies normal or unsafe network activities. These equations enable the LSTM to find network traffic patterns throughout time, which helps its anomaly detection capabilities.

$$P(y = Z|X) = \sigma(W_y.h_T + b_y) \quad (17)$$

The LSTM model identifies harmful actions in network traffic sequences through calculations made on h_T, which produces Z probability values. The weight vector W_y and bias b_y manipulate the information before applying the sigmoid activation function σ to generate a probability score. The system identifies network intrusions when a calculated probability level surpasses the defined threshold. The classification equation enables the model to evaluate and react to cyber threats in real time for instantaneous anomaly detection.

$$\theta^{new} = \theta^{old} + \lambda.(FP - FN) \quad (13)$$

The IDS enhances its accuracy over time by modifying the detection threshold θ using information from detected false positives (FP) and false negatives (FN). The IDS utilizes a control parameter λ known as the learning rate to adjust the threshold θ. An excessive number of FP triggers the system to boost θ to stop false detection of normal patterns. When FN increases by producing missed intrusions, the system decreases θ to enhance sensitivity. Through adaptive processes, the security framework maintains continuous development to detect new threats that emerge in WSNs.

IV. RESULT AND DISCUSSION

This section focuses on the performance analysis of IDS in WSN to identify cluster traffic as normal or more sensitive. The proposed method, ABC-LSTM, was compared with earlier approaches such as DNN, WOA-ABC, and FANN. The study evaluated several performance metrics, including throughput performance, Packet Delivery Ratio False Alarm Ratio execution time, and the rates of False Positives and False Negatives Table 1 presents the simulation parameters used in this study.

Table 1. Simulation parameters

Parameter Name	Values
No of Sensor Nodes	50-500
Packet Transmission Rate	10-100

Attack Types	Blackhole, Wormhole, DoS, Sybil, etc.
Used Software	NS-2 Simulator

The network includes between 50 to 500 sensor nodes responsible for data sensing and transmission duties inside their coverage region. The node-to-node communication occurs through packet transmission that operates between 10 and 100 packets per second for maintaining a continuous data stream for real-time analysis. The testing scenario consists of three different attack procedures: Blackhole, Wormhole, Denial-of-Service (DoS), and Sybil against WSN security vulnerabilities. The NS-2 serves as the platform to simulate real scenarios with accurate duplication of WSN behavior, attack effects, and ABC-LSTM intrusion detection performance assessment.

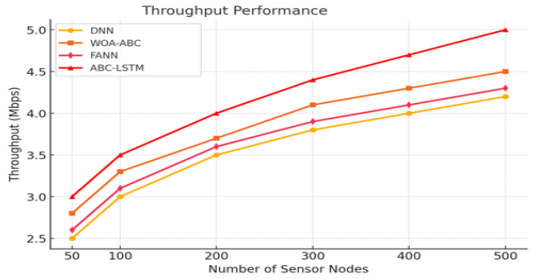

Fig. 2 Analysis of throughput performance

Figure 2 illustrates the throughput performance evaluation of IDS in WSNs, which compares DNN, WOA-ABC, and FANN algorithms with the proposed ABC-LSTM method. The ABC-LSTM model is the highest throughput solution thus making it an optimal selection for IDS frameworks that handle large-scale WSN deployments.

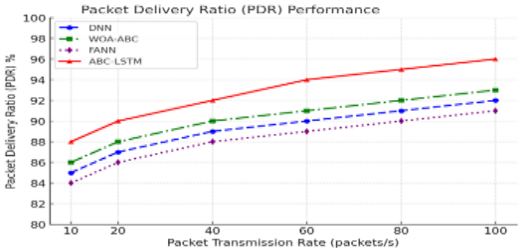

Fig. 3 Analysis of PDR performance

Figure 3 demonstrates the PDR performance evaluation of WSN IDS, which examines DNN, WOA-ABC, and FANN alongside the proposed ABC-LSTM approach. The PDR improves when packet transmission rates increase, while ABC-LSTM maintains the best PDR metrics throughout the process. The ABC-LSTM model delivers reliable communication because it has high PDR values, making it an effective IDS solution for big WSN networks.

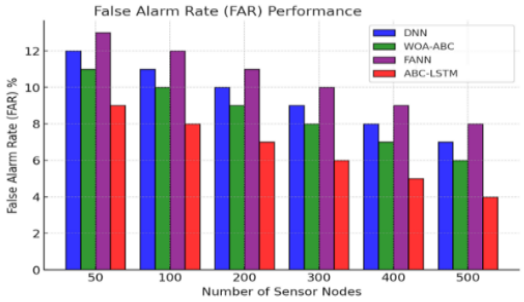

Fig. 4 Analysis of FAR performance

Figure 4 compares different IDS methodologies, including DNN, WOA-ABC, and FANN, regarding FAR performance analysis for WSNs to identify normal and malicious behaviors. According to all methods, increasing sensor nodes results in falling FAR values, while ABC-LSTM maintains the lowest FAR values. The lower ABC-LSTM model FAR enables enhanced security alerting, which reduces unnecessary disruptions, thus making it an efficient, reliable IDS for protecting large-scale WSNs.

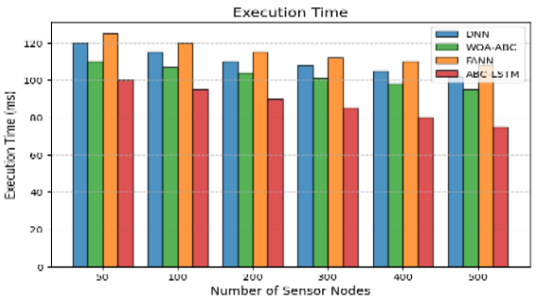

Fig. 5 Analysis of execution time performance

The figure 5 execution time performance analysis evaluates multiple IDS methods, including DNN, WOA-ABC, FANN, and ABC-LSTM, based on WSNs to determine their computational efficiency. ABC-LSTM demonstrates superior execution time performance because it achieves the shortest processing times when sensor nodes reach higher numbers due to its optimized hyperparameter tuning and enhanced processing efficiency. ABC-LSTM demonstrates its superior ability to reduce execution time efficiently, thereby providing an effective solution for intrusion detection in real-time, large-scale WSN security applications.

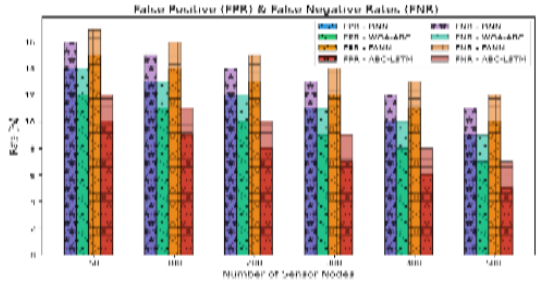

Fig.6 Analysis of FPR & FNR performance

A comparison between IDS effectiveness in WSNs is evident through the data in figure 6. This figure depicts the FPR and FNR performance results assessment between DNN, WOA-ABC, FANN, and the proposed ABC-LSTM model. FPR reports the proportion of legitimate activities IDS identifies as malicious, and FNR shows the percentage of actual attack events that the system labels normal. The effectiveness of an intrusion detection system rises as its values decrease for both metrics. The proposed ABC-LSTM model maintains the lowest FPR and FNR metrics to prove its exceptional accuracy for anomaly detection tasks.

V. CONCLUSION

The secure knowledge and cluster-based IDS implementing the ABC-LSTM method enhances WSN intrusion detection by combining LEACH-based clustering with ACO-based feature selection and ABC-LSTM-based intrusion detection methods. LEACH optimizes network efficiency and scalability through cluster organization because it cuts down communication overhead. Through its operation, ACO delivers better detection accuracy by selecting crucial cluster features, thus cutting down computational processing requirements. The ABC-LSTM model utilizes the ABC algorithm optimization to refine LSTM parameters because it enables adaptive and highly precise intrusion detection. The experimental results demonstrate that our method delivers better detection accuracy, heightened energy efficiency, and decreased false alarm probabilities over standard IDS solutions. The proposed IDS framework brings forth an efficient security solution that provides robustness, scalability, and energy-saving capabilities for WSNs.

REFERENCES

[1] Alsahli, M. S., Almasri, M. M., Al-Akhras, M., Al-Issa, A. I., & Alawairdhi, M. (2021). Evaluation of machine learning algorithms for intrusion detection system in WSN. International Journal of Advanced Computer Science and Applications, 12(5).

[2] Baraneetharan, E. (2020). Role of machine learning algorithms intrusion detection in WSNs: a survey. Journal of Information Technology, 2(03), 161-173.

[3] Ahmad, Z., Khan, A. S., Shiang, C. W., Abdullah, J., & Ahmad, F. (2020). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1), e4150. https://doi.org/10.1002/ett.4150

[4] J. Lansky et al., "Deep Learning-Based Intrusion Detection Systems: A Systematic Review," in IEEE Access, vol. 9, pp. 101574-101599, 2021, doi: 10.1109/ACCESS.2021.3097247.

[5] Singh, G., & Khare, N. (2021). A survey of intrusion detection from the perspective of intrusion datasets and machine learning techniques. International Journal of Computers and Applications, 44(7), 659–669.https://doi.org/10.1080/1206212X.2021.1885150

[6] H.Sadia et al.,"Intrusion Detection System for Wireless Sensor Networks: A Machine Learning Based Approach," in IEEE Access, vol.12, pp.5256552582,2024, doi:10.1109/ACCESS.2024.3380014.

[7] Gowdhaman, V., Dhanapal, R. An intrusion detection system for wireless sensor networks using deep neural network. Soft Comput 26, 13059–13067 (2022). https://doi.org/10.1007/s00500-021-06473-y

[8] Vembu, G., & Ramasamy, D. (2023). Optimized deep learning-based intrusion detection for wireless sensor networks. International Journal of Communication Systems, 36(13), e5254. https://doi.org/10.1002/dac.5254

[9] Sakthimohan, M., Deny, J., and Rani, G. Elizabeth. 'Secure Deep Learning-based Energy Efficient Routing with Intrusion Detection

System for Wireless Sensor Networks'. 1 Jan. 2024: 8587 – 8603. DOI: 10.3233/JIFS-235512

[10] Kagade, R. B., & Jayagopalan, S. (2022). Optimization assisted deep learning-based intrusion detection system in wireless sensor network with two-tier trust evaluation. International Journal of Network Management, 32(4), e2196. https://doi.org/10.1002/nem.2196

[11] Kasongo, S. M., & Sun, Y. (2020). A deep learning method with wrapper-based feature extraction for wireless intrusion detection system. Computers & Security, 92, 101752.https://doi.org/10.1016/j.cose.2020.101752

[12] L. Yang, J. Li, L. Yin, Z. Sun, Y. Zhao and Z. Li, "Real-Time Intrusion Detection in Wireless Network: A Deep Learning-Based Intelligent Mechanism," in IEEE Access, vol. 8, pp. 170128-170139, 2020, doi: 10.1109/ACCESS.2020.3019973.

[13] Talukder, M.A., Sharmin, S., Uddin, M.A. et al. MLSTL-WSN: machine learning-based intrusion detection using SMOTETomek in WSNs. Int. J. Inf. Secur. 23, 2139–2158 (2024). https://doi.org/10.1007/s10207-024-00833-z

[14] Hussain,K.,Xia,Y.,Onaizah,A.N.,Manzoor, T., & Jalil, K. (2022). Hybrid of WOA-ABC and proposed CNN for intrusion detection system in wireless sensor networks. Optik,271, 170145.https://doi.org/10.1016/j.ijleo.2022.170145

[15] Riyaz, B., Ganapathy, S. A deep learning approach for effective intrusion detection in wireless networks using CNN. Soft Comput 24, 17265–17278 (2020). https://doi.org/10.1007/s00500-020-05017-0