International Journal of Applied Mathematics

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ADAPTIVE INTRUSION DETECTION SYSTEMS FOR WIRELESS SENSOR NETWORKS: A HYBRID MACHINE LEARNING APPROACH

Ramesh Kait[1], Jyoti Saini[2], Ashish Girdhar[3]

[1,2,3]Kurukshetra University, Kurukshetra

rameshkait@kuk.ac.in[1], Jyoti.dcsa@kuk.ac.in[2], ashishgirdhar@kuk.ac.in[3]

Abstract:

Nowadays, Wireless Sensor Networks are growing rapidly and a considerable portion of telecommunication. Wireless sensor networks are made up of tiny, low powered sensor nodes, which perceive information from their surroundings., analyse them and connect to the sink nodes wirelessly, have limitations and security threats due to their low memory and computational power. As the network is growing rapidly, it is critical to detect malicious activities in network. For safeguarding the sensitive data from vulnerabilities, Intrusion Detection System (IDS) emerges as a crucial tool. Various studies focus on the improved accuracy of the intrusion detection model and a reduced false alarm rate. Due to this, the elimination of repeating features is demonstrated. This research presents a hybrid classification approach for identifying malicious network packets using a simulated network environment. Our hybrid model uses an intelligent feature selection process that improvise the utility of dataset by preprocessing the data and tuning the feature set by including only relevant feature in dataset. After removing the redundant features, a subset of 41 is selected and narrowed down to 20 pivotal features using Neighbourhood Component Analysis (NCA) for effective and efficient analysis. The study involves a comprehensive comparison of K-Nearest Neighbors, Decision Tree, and Ensemble classifiers, and introduces a hybrid method that integrates these classifiers on the basis of voting mechanism to enhance detection accuracy and robustness. Performance is evaluated using key metrics such as accuracy, precision, recall, F-measure, detection rate, and false alarm rate. Experimental results demonstrate that the hybrid model significantly outperforms individual classifiers, achieving higher detection rates and lower false alarm rates. This study underscores the efficacy of ensemble techniques and hybrid models in cybersecurity applications, providing a robust framework for intrusion detection. The implications of this research are profound, offering an impressive 99.24% of accuracy rate with very low False Alarm Rate. By significantly boosting the IDS accuracy and minimizing the false alarm rate, This study advances WSN's security posture against emerging cyber threats.

Keywords: Network Intrusion Detection, K-Nearest Neighbors, Decision Tree, Ensemble Methods, Hybrid Methods, Machine Learning, Cybersecurity

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

1. Introduction

Wireless Sensor Networks (WSNs) are a foundational aspect of modern wireless communication technologies, comprising nodes configured in various topological structures such as star, tree, or mesh. These sensor nodes are crucial for a range of functions including data sensing, processing, and communication. WSNs are extensively used in applications like environmental monitoring, security surveillance, and asset tracking, offering a cost-efficient and energy-saving solution for wireless communications [1]. However, the open nature of WSNs makes them susceptible to security threats from unauthorized entities, necessitating the implementation of robust security frameworks to protect the integrity of the network and its data [2].

In the realm of network infrastructure, Wi-Fi-based sensors are prevalent, facilitating global data accessibility via TCP/IP protocols on devices such as computers and smartphones. To extend the coverage beyond the range of a single Wi-Fi access point, repeaters can be used to enhance connectivity. These sensors utilize network identifiers (SSID) and passphrases to connect to the network and can transmit data directly to servers through URLs or IP addresses [3].

In order to secure the computers from the unwanted access Intrusion Detection systems (IDS) are very essential. These systems can be implemented in hardware or software forms and can be classified into network-based and host-based systems. Host-based IDSs are integrated into devices to monitor local activities, while network-based IDSs scrutinize network traffic to identify suspicious activities [4].

IDS technologies classify potential threats into categories such as Normal, Flooding, Injection, and Impersonation using datasets like the Aegean Wi-Fi Intrusion Dataset (AWID) [5]. The methods of attack detection are generally divided into four types: anomaly-based, which detects new, unusual patterns of behavior; signature-based, which recognizes known threats via predefined signatures; specification-based, which monitors deviations from normal operations in network configurations; and hybrid-based, which combines the features of the other three types to enhance detection capabilities [6].

The adaptability, accessibility, and mobility provided by wireless networks offer substantial advantages over traditional wired networks, eliminating the need for extensive physical infrastructure [7]. Wireless IDS (WIDS) are specialized tools designed to sense and protect wireless local area networks (WLANs) by continuously checking for signs of network breaches [8].

Intrusion detection plays an essential role in securing WSNs by detecting and minimizing harmful activities [9]. Traditional IDS that use static rules or thresholds can be inadequate for dealing with sophisticated and changing threats [10]. Machine Learning (ML) methods offer a powerful solution for improving the security of WSNs. These algorithms analyse past data to detect irregularities and patterns indicating possible security breaches, enabling more dynamic and preventive security measures [11]. ML techniques, WSNs can develop sophisticated IDS

Received: August 07, 2025

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

capable of sifting through extensive data to spot unusual patterns and differentiate between benign and harmful activities [12]. Algorithms including decision trees (DT), random forests, neural networks, and gradient boosting are especially potent, providing deeper insights and boosting the accuracy and effectiveness of IDS in WSNs [13].

ML techniques and Neural Network Techniques are used for estimation purpose as well as for network security involve training models on labeled data to distinguish between normal and malicious activities[14]. This paper compares four ML approaches: K-Nearest Neighbors (KNN), Decision Tree, Ensemble methods, and a Hybrid approach. KNN classifies data based on the group decision, balancing simplicity and ease of implementation but facing challenges with high-dimensional data. DT, which recursively split data based on feature values, are powerful and interpretable but prone to overfitting. Ensemble techniques, such as bagging and boosting, integrate various models to enhance precision and reliability, though they tend to be intricate and demand significant computational resources. This paper evaluates four different ML techniques for network intrusion detection: KNN, DT, Ensemble methods, and a Hybrid approach. Through simulation of a network environment and assessment of these methods, the goal is to determine the most efficient strategy for real-time network security. The Hybrid approach leverages multiple classifiers to enhance overall performance by mitigating individual weaknesses.

A. Problem Statement

There is various security threats present in the WSN particularly in discovering and neutralizing the malicious nodes or attackers. It is difficult to identify any malicious or attacking node quickly and accurately for intrusion detection in WSN. IDS efficiency is crucial for prompt identification and immediate corresponding action specifically in wireless kind of networks which have limited energy and are very prone to attacks. These attacks include: anomaly-based attacks, signature-based attacks, specification-based attacks, and DoS attacks etc. This investigation aims to contribute for strengthening the WSN by evolution of IDS technologies. In addition to navigate the complex issue in WSN's security, the objective is to open the doors for more future innovations in IDS.

B. Contribution

This research offers multiple important advancements in the area of network intrusion detection, especially within WSNs. It introduces a hybrid classification approach that combines the strengths of KNN, DT, and Ensemble methods. This hybrid method enhances the robustness and accuracy of packet classification in network environments by leveraging majority voting from multiple classifiers. This research also helps in developing a comprehensive simulation framework that mimics a network environment with normal and malicious packets. The framework includes mechanisms for simulating packet transmission, interception by attackers, and classification using various ML models. This Provided a detailed performance evaluation of the classification models using standard metrics such as accuracy, recall, detection rate, F-measure and false alarm rate. This thorough assessment allows for a clear comparison of the effectiveness of different classifiers in detecting network attacks. It Implements multiple

Received: August 07, 2025

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

classifiers (KNN, DT, and Ensemble) and demonstrated their integration within a single system. This integration showcases the potential for combining different algorithms to achieve better performance in real-world applications. The contributions highlight the potential for using ML techniques to enhance the security and reliability of network communications. This research has the following major contributions:

- Identifying Key Features of NSL-KDD Datasets for Intrusion Detection in WSN.
- By focusing on most discriminative features, the study optimizes performance using advanced feature scaling and selection, which result a feature set of 41 and 20 dimensions.
- For model efficiency improvement multiclass dataset is converted into binary labels in enhancing model training.
- The study also analyses the effectiveness of different ML Models including KNN, DT and ensemble learning.
- A Group Decision based hybrid framework is designed by combining all fitted models like KNN, DT and Ensemble Learning models for enhancing the accuracy and reliability of the network.
- Multiple performance metrices such as Accuracy, Precision, Recall, FMeasure, Detection Rate and False Alarm Rate are used to assess the proposed hybrid model's effectiveness.

The organization of the paper is structured as follows: Section 2 surveys related literature. Section 3 describes the proposed methods. Section 4 examines the experiments and their results. Section 5 compares these results to existing advanced techniques. Section 6 summarizes the key findings, while Section 7 explores potential areas for future research.

2. Related Works

Research on intrusion detection inside WSNs has grown in importance as the frequency of attacks on WSNs keeps rising. This work investigates many ML models for intrusion detection, especially those meant to improve security in WSNs. Models intended primarily to identify potential risks and anomalies in sensor data and network traffic take center stage. The performance of these models determines whether unauthorized access can be stopped as well as if data sent via sensor networks guarantees security and privacy.

Table 1 The existing literatures based on ML methods and datasets used

Author's Name	Objectives	Dataset	Techniques	Outcome	Remarks
Abdullah et al.	Examination of Denial of Service (DoS) attacks	WSN-DS	Classifiers assessed were Naive Bayes, Random Forest, Support Vector Machine	SVM classifier outperformed others with an outstanding detection rate of 96.7%	WEKA data mining methods were used

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

			(SVM), and J48		
Tan et al. [15]	To improve pattern discovery performance in datasets with unbalanced class distributions	KDD Cup 99 dataset	Synthetic Minority Oversampling Technique (SMOTE), Random Forest	The dataset is balanced using SMOTE and after applying SMOTE the accuracy of RF increased from 92.39% to 92.57%	Study focuses only on RF, other ML algorithms could be explored like SVM, Neural Networks, or Gradient Boosting for broader understanding and performance comparison.
Shaima a Ahmed Elsaid et al. [16]	Developed an optimized collaborative Intrusion Detection System (OCIDS) for WSNs	NSL-KDD	SVM	97.9% average detection rate is achieved with a small standard deviation 0.9%.	A thorough analysis is conducted to evaluate various attack scenarios.
Md Alaudd in Rezvi et al. [17]	To explore and evaluate various data mining approaches for DoS attacks in WSNs.	WSN-DS	KNN, Naïve Bayes, Logistic Regression, SVM and ANN algorithms	No single algorithm outperformed while analysing. However, Logistic Regression consistently performed better in most cases.	The outcomes show the effectiveness of machine learning techniques, particularly Logistic Regression, in detecting DoS attacks in WSNs, while also emphasizing the need for strategies to manage class imbalance in datasets.

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Shashank Gavel et al. [18]	To address the security issues faced by Wireless Networks (WNs)	NSL-KDD, AWID	Optimized Maximum Correlation based Feature Reduction (OMCFR), Random Forest	Study showed beneficial findings with High detection rate and reduced false positive rates(FPR) .	Only few performance parameters are used for result evaluation. More performance metrices like precision, recall, F-Measure could be included.
Sung Bum Park et al. [19]	Security improvements of Controller Area Network (CAN) using Graph-IDS	Intrusion Detection Dataset for Car Hacking	Graph theory, Threshold based-IDS	The attack detection rate is reached more than 90% while comparing to other existing alogorithms.	The research opens the doors for applying graph theory for the security of connected vehicles
Irfan Ali Kandhro et al. [20]	Enhancing cybersecurity measures in IoT environments	KDDCup99, NSL-KDD, and UNSW-NB15	Generative Adversarial Networks (GANs):	Enhanced detection rate resulting between 95-97% of attacks and intrusions in IoT environments	The study highlights significant challenges in effectively extracting and utilizing relevant features for attack detection
Chaya Ravindra et al.[21]	To develop an effective method for detecting anomalies in WSNs	IBRL	Extreme Learning Machine (ELM)	Attained an impressive overall accuracy of 97.4%	ETELMAD shown significant results while detecting anomalies in WSNs compared to other existing techniques.
Periasamy Nancy et al. [22]	To improve the security of WSN using advanced IDS.	KDD CUP and Network Trace Dataset	Fuzzy Temporal DT integrated with CNN	Network performance enhanced	More performance metrices should be included for results.

Received: August 07, 2025

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

U Nandhini et al.[23]	Enhance the Performance of Network Intrusion Detection System (NIDS)	NSL-KDD	Two stage classification using SVM and KNN	95.01% overall accuracy is achieved	Future improvements can be done to improve intrusion detection accuracy
Harun Bangali et al.[24]	To detect Middle Box Attack	IoHT	Ranking subset and CNN	Results revealed the significance of this methodology over other existed models.	Proposed methodology outperformed the existing approaches.
K. Yesodha et al.[25]	To develop an effective IDS	NSL-KDD and real time data from sensor nodes	Fuzzy Temporal rules with Artificial Bee Colony (ABC) and CNN	Enhanced Accuracy and decreased FPR	The proposed IDS may face challenges when deployed to a network with large number of sensors
Kannan A et al.[26]	Identification and isolation of RPL attacks	NSL-KDD	Neural Networks and Genetic Algorithms based classification Algorithm	RPL attacks are reduced in routing process with improved detection rate	Proposed approach shown significant improvement when compared to other existing approaches
Shalini Subramani et al.[27]	IDS for IOT sensor networks	Data collected from the MATLAB simulator of sensor network trace	Fuzzy Temporal Random Forest algorithm	Improved Detection Accuracy by 5% with reduced FPR	The proposed IDS was assessed in a controlled environment, which is crucial for validating its effectiveness.
Shalini Subramani et al.[28]	Feature Selection for IDS in WSNs	NSL-KDD19, KDD'99 Cup,CIDD	PSO, Multiclass SVM	Average precision of 89.93%, an average recall of 83.825 is measured as results	More Performance evaluation metrices should be incorporated

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Existing literature is surveyed in *Table 1* on the basis of techniques and methods used for the IDS and other security issues. Various ML and optimization techniques are used to achieve the objective of the research. The remarks column of the table shown the limitations and achievements of that research. From the table we can analyze the great work has been done in the area of security issue of the WSN and Various models for Intrusion Detection are designed and developed by the researchers. Too high packet delivery ratios is still big issue for researchers. Mostly the researchers focus on the performance parameters like accuracy and FPR only for considering in their evaluation and not achieving the performance on more than three or four parameters on the same level is also an issue to deal with.

There are some optimization-based models are presented by S. Rajasoundaran et al.[29]and youxiang Duan[30] shown the optimization-based algorithms for WSNs those can be incorporated for the optimization purpose.

3. Proposed Methodology

The proposed method is for developing a group decision-based hybrid IDS for WSNs for the detection of various types of intrusions and attacks in the network. Machine Learning approach is used in this research due to their exceptional capabilities of feature extraction, feature engineering and pattern recognition. They are very much accurate in identifying the malicious activities in the network. Furthermore, advance feature scaling and selection methods are applied, which results a feature set of 41 and 20 dimensions. This approach is also evaluated in comparison of other techniques like DT, KNN and ensemble learning and results shown proposed methodology more effective. Our decision-making process is grounded in scientific principles and give better results from majority. The proposed method integrates three key phases: preprocessing, feature engineering, and classification. An embedded feature selection method is applied for identifying the most contributed features for more accurate predictions. The primary steps of our model include:

- Preprocessing the NSL-KDD dataset
- Applying feature selection and reduction
- splitting the dataset for classification
- Applying Group Decision Based Hybrid ML model for intrusion detection
- Evaluating the results for continuous improvement.

Figure 1 illustrates the structured process used for intrusion detection in WSNs, beginning from data collection to the final prediction stage. The process starts with gathering a comprehensive dataset that includes network traffic and sensor data. This raw data undergoes preprocessing to rectify issues like missing values, noise, and inconsistencies, preparing it for detailed analysis. Subsequently, feature scaling is implemented to normalize the data, and feature selection techniques are used to isolate the most critical features, thereby boosting the efficiency and accuracy of the models. The refined data is then split into training and testing sets. Hybrid model (group decision based on voting mechanism of models KNN, DT & Ensemble methods) is trained using the training dataset. This proposed model is then evaluated using the testing

Received: August 07, 2025

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

set, and their predictions are integrated through a voting mechanism to determine the final outcome, ensuring effective and precise intrusion detection. The process is outlined in detail below:

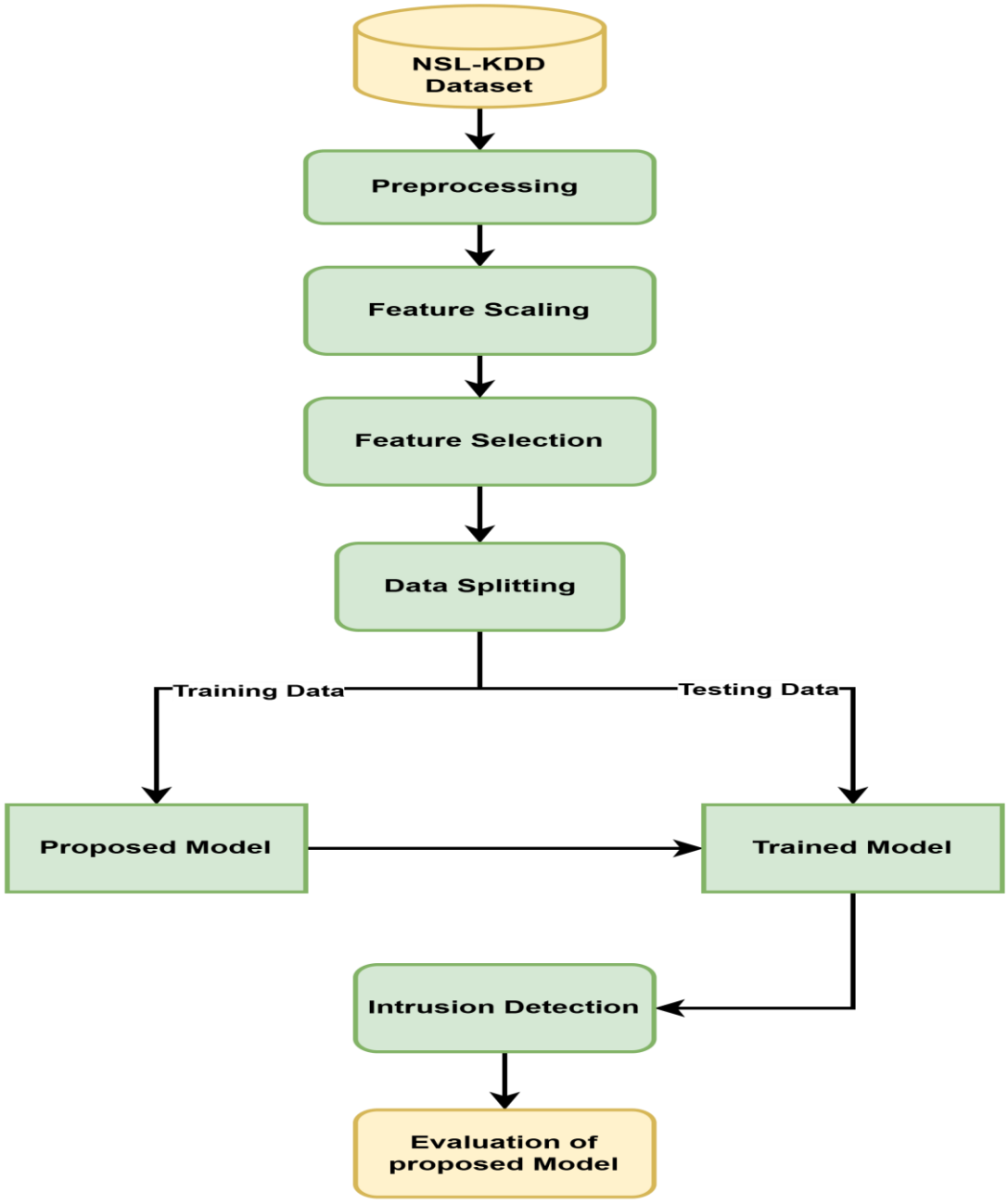

Figure 1 Proposed Hybrid ML Model for IDS in WSN

3.1 Data Preprocessing

Preprocessing of data is a major and essential step in the preparation of our dataset for effective analysis and model building. This section outlines the specific preprocessing methods employed to ensure data quality and suitability for further processing. This process is shown in ***Figure 2*** and involves transforming raw data from the NSL-KDD dataset into a refined format

Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

compatible for ML models. Key steps in this process include data cleaning, where errors and inconsistencies in the Dataset, particularly in the training as well as in testing subsets, are corrected, as shown in Figure 2. Scaling, Normalization, and Potential Feature Engineering are all the part of data transformation, which is converting the data into the most suitable format for ML models. For effective and accurate intrusion detection in WSNs, this preprocessing process guarantees training and testing of ML models on high-quality, relevant data.

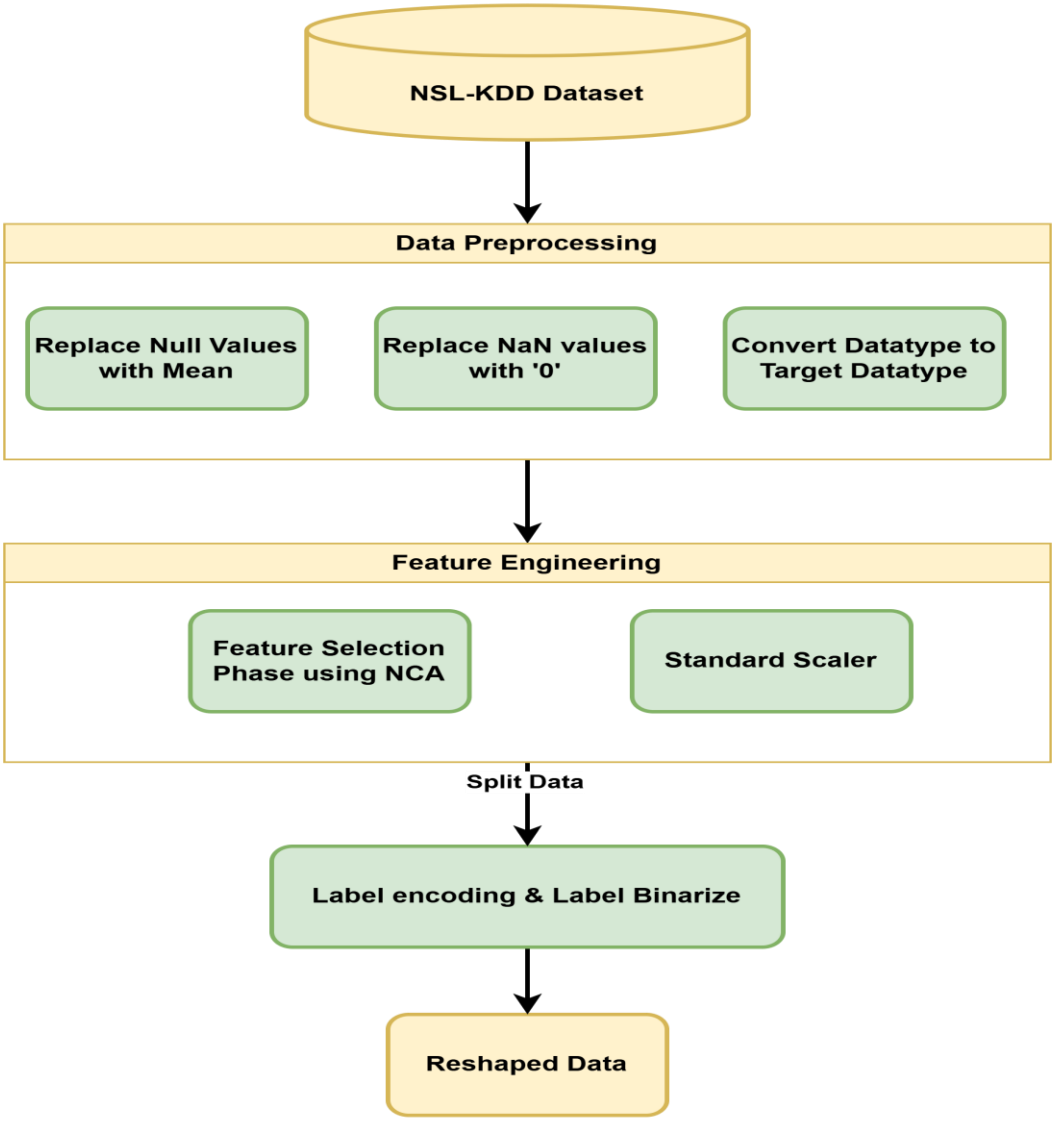

Figure 2 Data Preprocessing

3.1.1 Handling Null Values

Null values in a dataset can disrupt analysis and model training as they represent missing information. Replacing null values with that particular column's mean value helps maintain the dataset's integrity without distorting its statistical properties. This approach ensures that the overall distribution of the data is preserved.

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Given a dataset D consisting of n observations and m features, we represent it as a matrix $D = [X_{ij}]$ where i denotes the observation index (from 1 to n) and j denotes the feature index (from 1 to m).

- Identify Null Values: Let N_{ij} denote the presence of a null value in X_{ij}:

$$N_{ij} = \begin{cases} 1 & \text{if } X_{ij} \text{ isnull} \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

- Replace Null Values with Mean**:** Calculate the mean μ_j for each feature j:

$$\mu_j = \frac{\sum_{i=1}^{n} X_{ij} \cdot (1 - N_{ij})}{\sum_{i=1}^{n} (1 - N_{ij})} \quad (2)$$

Replace X_{ij} with μ_j if $N_{ij} = 1$:

$$X_{ij} = \begin{cases} \mu_j & \text{if} N_{ij} = 1 \\ X_{ij} & \text{otherwise} \end{cases} \quad (3)$$

Equation (1) identifies the Null values N_{ij} from the data. Mean μ_j calculated in equation (2). Then those Nullvalues are replaced by mean. Then equation (3) shows how the Null values are replaced by mean in the data.

3.1.2 Handling NaN Values

NaN (Not a Number) values can cause computational errors or lead to misleading results in numerical computations. Replacing NaN values with 0 ensures that the dataset remains compatible with algorithms that do not support NaN handling and avoids disruptions during analysis or model training.

- Identify NaN Values**:** Let K_{ij} denote the presence of a NaN value in X_{ij}:

$$K_{ij} = \begin{cases} 1 & \text{if} X_{ij} \text{isNaN} \\ 0 & \text{otherwise} \end{cases} \quad (4)$$

- Replace NaN Values with 0**:** Replace X_{ij} with 0 if $K_{ij} = 1$:

$$X_{ij} = \begin{cases} 0 & \text{if} K_{ij} = 1 \\ X_{ij} & \text{otherwise} \end{cases} \quad (5)$$

Equation (4) identifies the presence of NaN values in the data. Then all NaN values are replaced by 0 in equation (5).

3.1.3 Conversion of Data Types

It is crucial to verify that each column in a dataset matches the correct data type for effective and precise analysis or model training. Converting data to the appropriate types is key to meeting the needs of different ML algorithms, which can lead to better performance and easier interpretation of results.

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- Identify Data Types: Determine the current data type of each feature j. Let T_j be the target data type for feature j (e.g., integer, float, string).
- Convert Data Types: Convert X_{ij} to the target data type T_j:

$$X_{ij} \rightarrow T_j(X_{ij}) \tag{6}$$

In equation (6) $T_j(X_{ij})$ denotes the conversion of X_{ij} to the type T_j.

Applying these theoretical and mathematical steps, we ensure that the dataset D is preprocessed with no null or NaN values and all features are converted to the appropriate data types. This preparation is critical for the subsequent stages of analysis and ML model training, leading to more reliable and accurate outcomes.

3.2 Feature selection

Neighbourhood Component Analysis (NCA) learns a linear transformation (represented as a weight matrix) applied to the feature vectors to enhance the class separability. This transformation is learned by optimizing a loss function that reflects the differential contributions of the features to the classification accuracy. The implementation of NCA for feature selection can be structured into a sequence of clear, actionable steps, as outlined in Algorithm 1.

ALGORITHM 1: FEATURE SELECTION USING NCA

1 ***Computing Size and Unique Labels:***

Calculate the size of the feature set and the unique labels in your dataset.

2 ***Feature Selection:***

NCA to determine the relevance of each feature. A threshold is defined (mean of the feature weights scaled by 0.1 in your case), and features exceeding this threshold are selected for the final model.

3 ***Saving Selected Features:***

Post selection, the relevant features and labels are saved for further use.

The use of NCA for feature selection in ML allows for automatic selection of the most relevant features which improves the model's prediction accuracy and reduces overfitting by eliminating irrelevant or redundant features. This approach is particularly useful in scenarios where interpretability and computational efficiency are critical.

Standard Scaler

Machine Learning function is used in preprocessing and features scaling of training and testing datasets. Feature scaling is the important step for modelling, done by normalization before

Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

training, because it helps to select features with more weight at the time of result and convert the data points into the 0-1 range.

3.3 Label Encoding & Binarize

While some of the labels may not need the information to be arranged in a certain sequence (ordinal features), others may (nominal features). The names of the ordinal and nominal features belong to a string-based category set. Labels must be encoded as the integers at preprocessing stage only in order to accurately interpret the data by learning models. Label encoder assign values to the labels using a numeric encoding scheme. Label binarize assign binary classification against labels.

3.4 Proposed Hybrid Method

Figure 3 shows the architecture of proposed hybrid model. The tuned and pre-processed data is then divided into two parts: one for training the model and one for testing purpose. Then the data is fed to the model for experiment and evaluating the performance

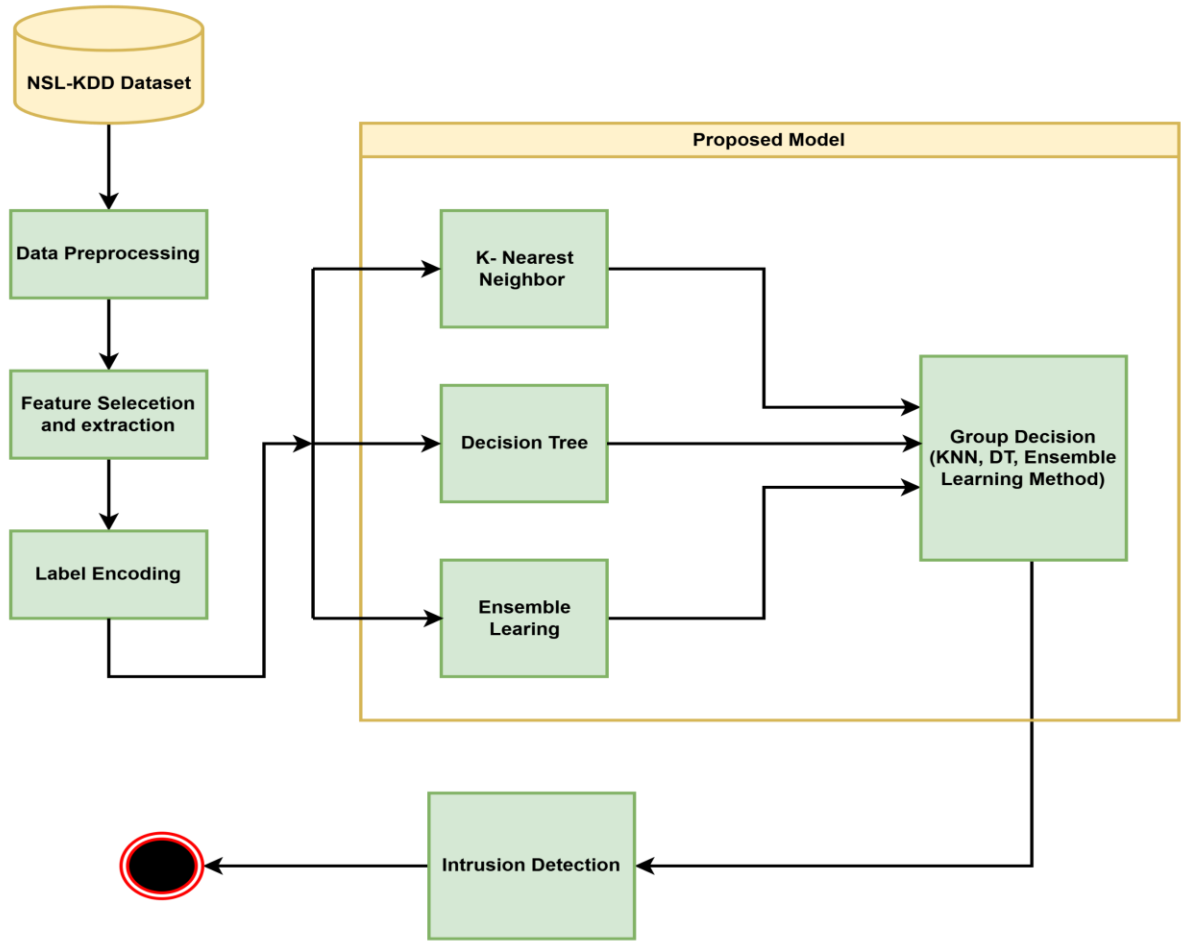

Figure 3 Architecture of Proposed Hybrid Model

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

KNN is an instance-based ML approach in which data point is classified on the basis of its distance to the k closest data points in the training set, often employing a metric like Euclidean distance [23]. Given a data point a and a training set with data points a_i and their corresponding labels b_i:

$$d(a, a_i) = \sqrt{\sum_{j=1}^{n} (a_j - a_{ij})^2} \tag{7}$$

The predicted label $\hat{b}$ is:

$$\hat{b} = \text{mode}(b_{i1}, b_{i2}, \dots, b_{ik}) \tag{8}$$

In equation (7) $d(a, a_i)$ (the distance between a and a_i) is calculated and mode returns the most frequent class label among the k nearest neighbors in equation (8).

DT is a flowchart-like diagram where internal nodes represent features, branches correspond to decision rules, and leaf nodes indicate class labels. The tree is constructed by repeatedly splitting feature values based data, with the objective of reducing impurities and improving information gain [31] The tree splits the data into regions R_j based on decision rules calculated in equation (9):

$$\hat{b} = \sum_{j=1}^{J} \hat{c}_j \mathbf{1}(a \in R_j) \tag{9}$$

In equation (10) $\hat{c}_j$ is the predicted class for region R_j, and $\mathbf{1}$ is an indicator function that is 1 if $a \in R_j$ and 0 otherwise.

Information Gain:

$$IG(S, F) = H(S) - \sum_{v \in \text{Values}(F)} \frac{|S_v|}{|S|} H(S_v) \tag{10}$$

where $H(S)$ is the entropy of the set S, F is the attribute, $\text{Values}(F)$ are the possible values of F, and S_v is the subset of S where F has value v.

Ensemble methods enhance classification performance by aggregating predictions from several base models. Key types of ensemble techniques include bagging, boosting, and stacking [32]. The ensemble prediction is the majority vote or weighted average of the base learners' predictions:

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$\hat{b} = \text{mode}(\hat{b}_1, \hat{b}_2, \dots, \hat{b}_M) \quad (11)$$

In equation (11) $\hat{b}_i$ is the prediction from the i-th base learner, and M is the total number of base learners.

Proposed Hybrid Method aggregates predictions from multiple classifiers (KNN, DT, Ensemble) using a voting mechanism to improve robustness and accuracy. The hybrid prediction is the majority vote among the classifiers' predictions and is called Group Decision:

ALGORITHM 2: PROPOSED HYBRID METHOD

for td in Testdata

out = zeros(1,NC)

for CL_i in NC

P_i=predict(CL_i, td)

out(P_i)=out(P_i)+1

end

[mx,idx]=max(out)

predict td=idx

end

Where Testdata=Data provided for testing

out = array initialized with zeros

NC = NumClasses (Attack/Non Attack)

CL_i= Classifier

P_i=Prediction

Proposed Hybrid Method provides a comprehensive framework that uses **Group Decision Mechanism** and enhances predictive performance through a synergistic combination of different ML techniques. This approach not only improves the accuracy and robustness of the predictions but also offers a scalable solution to tackle the intricacies of varied and complex datasets. This method combines the outputs of the different models (KNN, DT, and Ensemble method) by aggregating their predictions. Group Decision can be done through various techniques such as majority voting, weighted voting, or averaging. This step ensures that the final prediction is more robust and reliable, leveraging the strengths of all individual models.

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3.5 Prediction Output

The final step is to predict the output using the aggregated results from the voting mechanism. This output is the prediction of network traffic categorization as attack or non-attack, providing a robust IDS capable of improving the security of WSNs. The hybrid method involves simulating a network environment where packets are transmitted from senders to a receiver, potentially intercepted by attackers. It leverages multiple classifiers to predict whether a packet is normal or malicious. The hybrid method, which combines predictions from different classifiers, aims to maximize the overall accuracy and robustness of the classification process. Each classifier's performance is assessed using standard metrics, providing a comprehensive assessment of their effectiveness in detecting network attacks.

4 Experiment and Performance Analysis

In this section, we discuss the dataset used in our hybrid model, the performance metrics, and the performance analysis.

4.1 Dataset

This study utilizes the NSL-KDD dataset [33]. NSL-KDD is a standard dataset which is mostly used for testing IDS. Data is divided into two sets: training (80%) and testing (20%). The NSL-KDD dataset is chosen for its comprehensive inclusion of various types of network intrusions as well as normal traffic, making it an ideal resource for evaluating the effectiveness of intrusion detection models.

4.2 Performance Metrics

This section discusses the metrics used to assess the performance of the proposed hybrid intrusion detection model, as detailed in study [34]:

Accuracy: This metric indicates the proportion of total predictions that were correctly identified by the model. It is calculated using the formula:

$$\text{Accuracy} = \frac{(\text{TP}+\text{TN})}{(\text{TP}+\text{TN}+\text{FP}+\text{FN})} \times 100 \tag{13}$$

Precision: This measures the accuracy of positive predictions made by the model and is defined as:

$$\text{Precision} = \frac{\text{TP}}{(\text{TP}+\text{FP})} \times 100 \tag{14}$$

Recall (Sensitivity): Also known as sensitivity, this metric evaluates the model's ability to identify all relevant instances correctly:

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$\text{Recall} = \frac{\text{TP}}{(\text{TP}+\text{FN})} \times 100 \tag{15}$$

F-Measure (F1 Score): The harmonic mean of precision and recall, providing a balanced measure of the model's accuracy:

$$\text{F} - \text{Measure} = \frac{2\times\text{Precision}\times\text{Recall}}{(\text{Precision}+\text{Recall})} \times 100 \tag{16}$$

False Alarm Rate: Indicates the proportion of false positives relative to the total number of negative instances, a critical measure for evaluating the model's specificity:

$$\text{FalseAlarmRate} = \frac{\text{FP}}{(\text{FP}+\text{TN})} \times 100 \tag{17}$$

These metrics collectively from equation (13) to equation (17) provide a comprehensive evaluation of the model's performance, demonstrating its effectiveness in detecting and addressing cybersecurity threats.

4.3 Performance Analysis

The performance evaluation of the NIDS models utilizes a variety of metrics, including Accuracy, Precision, Recall, F-Measure, Detection Rate, and False Alarm Rate, to gauge the models' effectiveness.

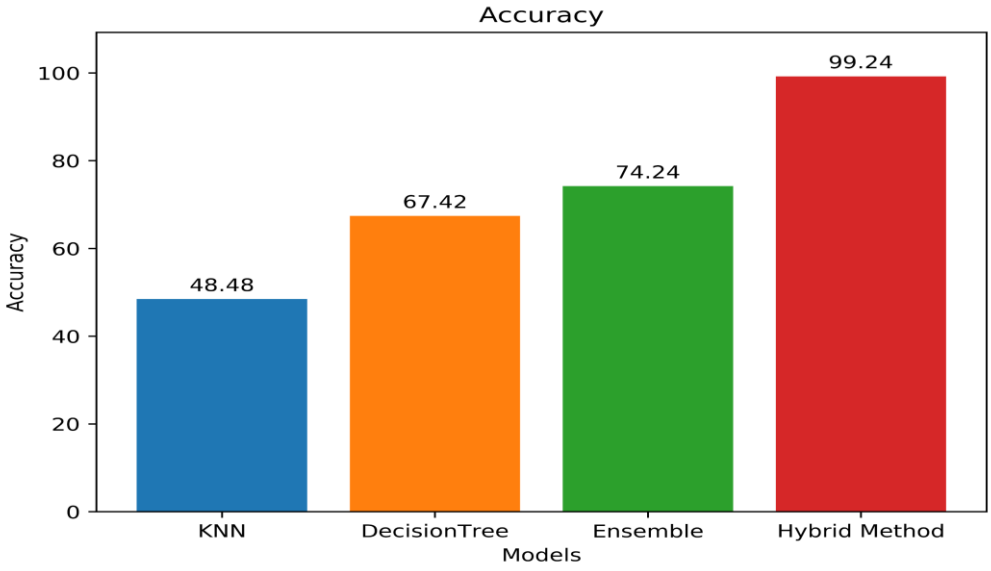

Figure 4 Comparative Analysis for Accuracy

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

In ***Figure 4*** , the KNN model records the lowest accuracy at 48.48%. This lower performance is attributed to its simplistic methodology and susceptibility to the complexities of high-dimensional data. In contrast, the DT model shows significant improvement, achieving an accuracy of 67.42%, thanks to its ability to capture non-linear relationships within the dataset. Further enhancement is observed with the Ensemble method, which attains an accuracy of 74.24%. This method boosts detection capabilities by combining predictions from multiple models, thereby increasing the system's robustness and generalization ability. The most notable performance is achieved by the Hybrid Method, which significantly outperforms all other models with an accuracy of 99.24%. This outstanding result highlights the Hybrid Method's advanced ability to combine the strengths of various algorithms, offering a highly efficient approach to network intrusion detection.

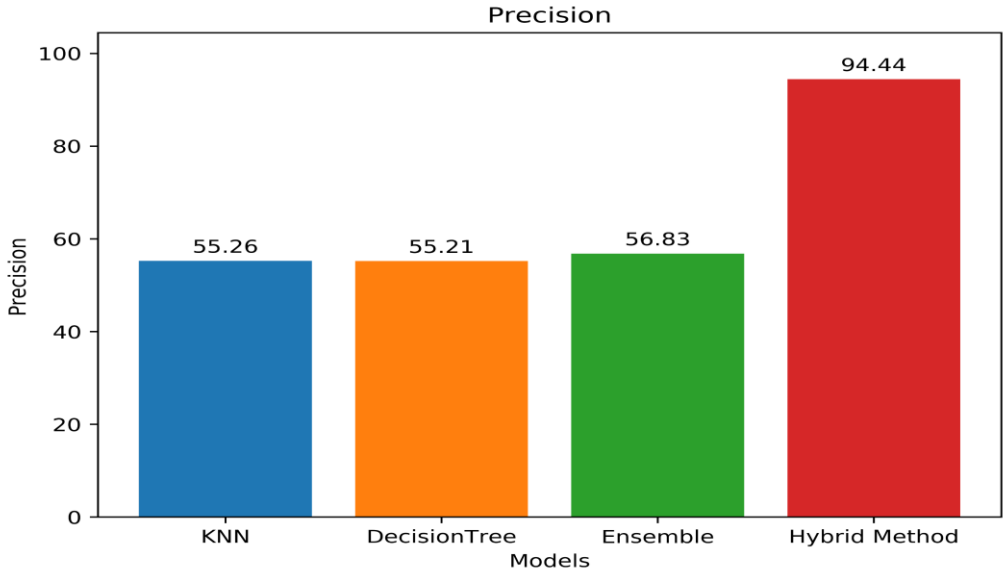

Figure 5 Comparative Analysis for Precision

In ***Figure 5,*** the precision analysis of NIDS models reveals varying effectiveness in accurately identifying true positive intrusions while minimizing false positives. Both KNN and DT models show similar and modest precision, indicating their limitations in consistently differentiating between normal and intrusive network activities. The Ensemble method demonstrates a slight improvement by harnessing the combined strengths of multiple models, resulting in better precision. However, the Hybrid Method stands out significantly, exhibiting exceptional precision.

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

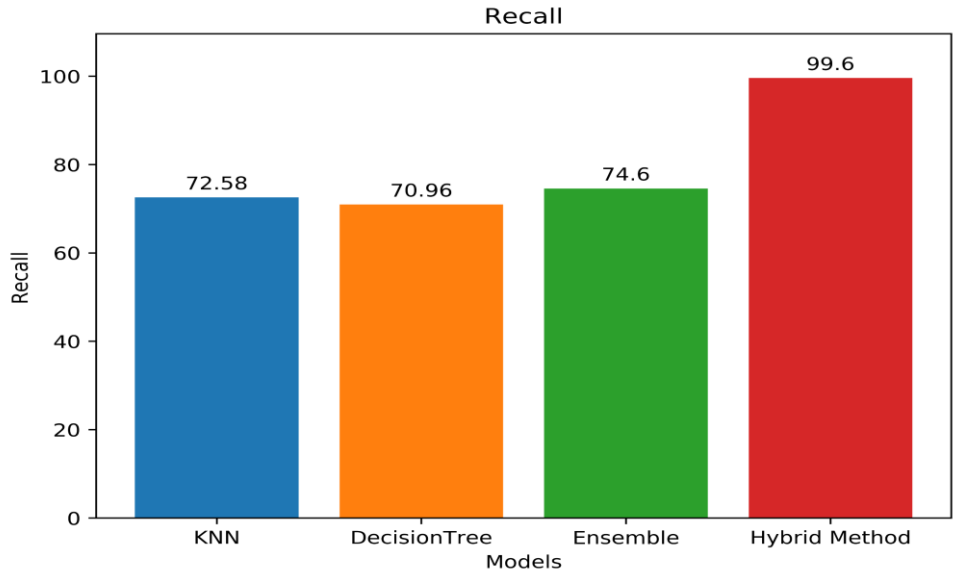

Figure 6 Comparative Analysis for Recall

In ***Figure 6***, the analysis of NIDS models based on recall highlights their effectiveness in identifying actual intrusions. The KNN model demonstrates relatively high recall, reflecting its ability to detect a substantial proportion of true intrusions. The DT model shows slightly lower recall, indicating some limitations in capturing all intrusions. The Ensemble method achieves a modest improvement in recall by leveraging the strengths of multiple models. However, the Hybrid Method excels with exceptionally high recall, showcasing its superior capability in detecting nearly all actual intrusions, making it the most comprehensive model for identifying true positives among those compared.

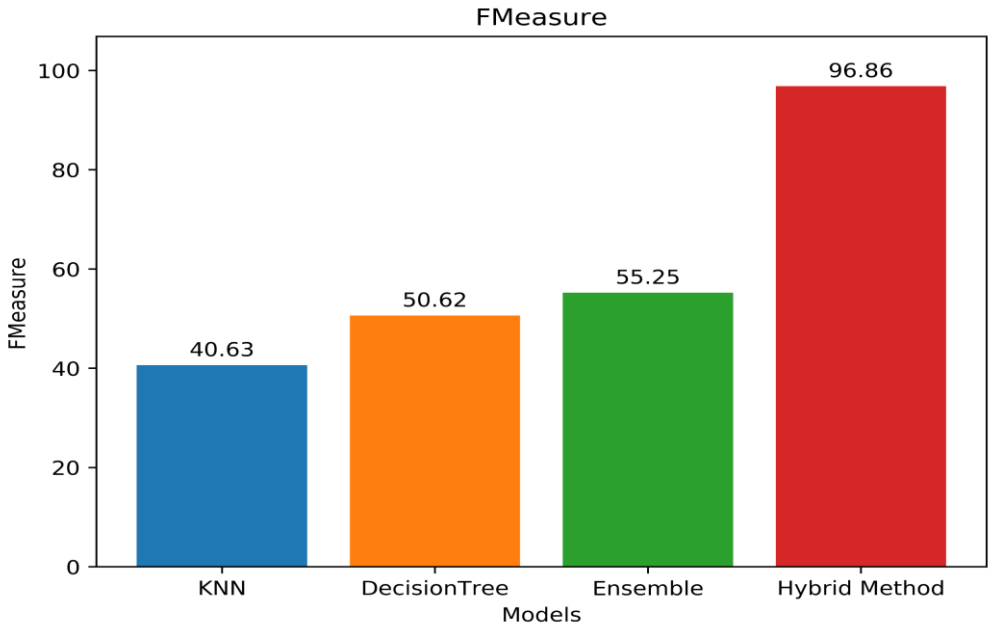

Figure 7 Comparative Analysis for FMeasure

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

In ***Figure 7***, the analysis of NIDS models based on the F-measure, which balances precision and recall, shows varying degrees of effectiveness. The KNN model has the lowest F-measure, reflecting its overall inefficiency in both detecting true intrusions and minimizing false positives. The DT model performs better, yet still shows limitations in achieving a balanced performance. The Ensemble method improves further, indicating a more balanced and robust detection capability. However, the Hybrid Method stands out with a remarkably high F-measure, demonstrating its superior ability to accurately and reliably identify network intrusions while maintaining a low false positive rate, making it the most effective model among those evaluated.

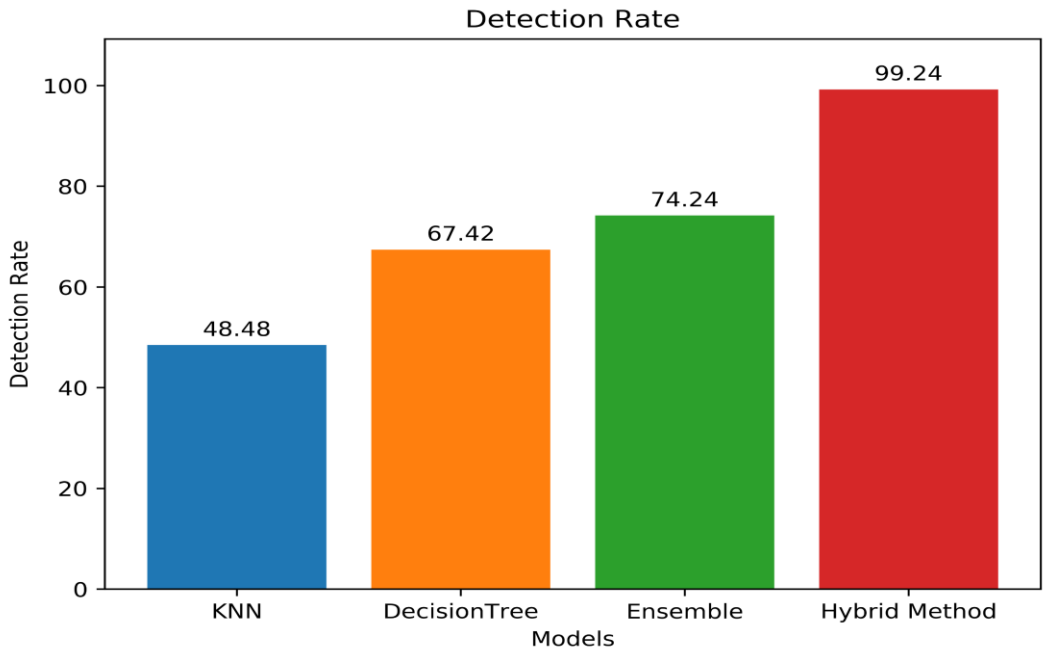

Figure 8 Comparative Analysis for Detection Rate

In ***Figure 8***, the evaluation of NIDS models based on their detection rates highlights the varying levels of effectiveness among the different approaches. The KNN model shows the lowest detection rate, indicating its relative ineffectiveness in precisely identifying intrusions. Conversely, the DT model marks a substantial improvement, achieving a higher detection rate due to its adeptness at managing complex data structures. The Ensemble method further boosts the detection capabilities by combining the strengths of various models, thereby enhancing overall robustness. However, it is the Hybrid Method that stands out the most, significantly surpassing the other models with its exceptional detection rate.

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

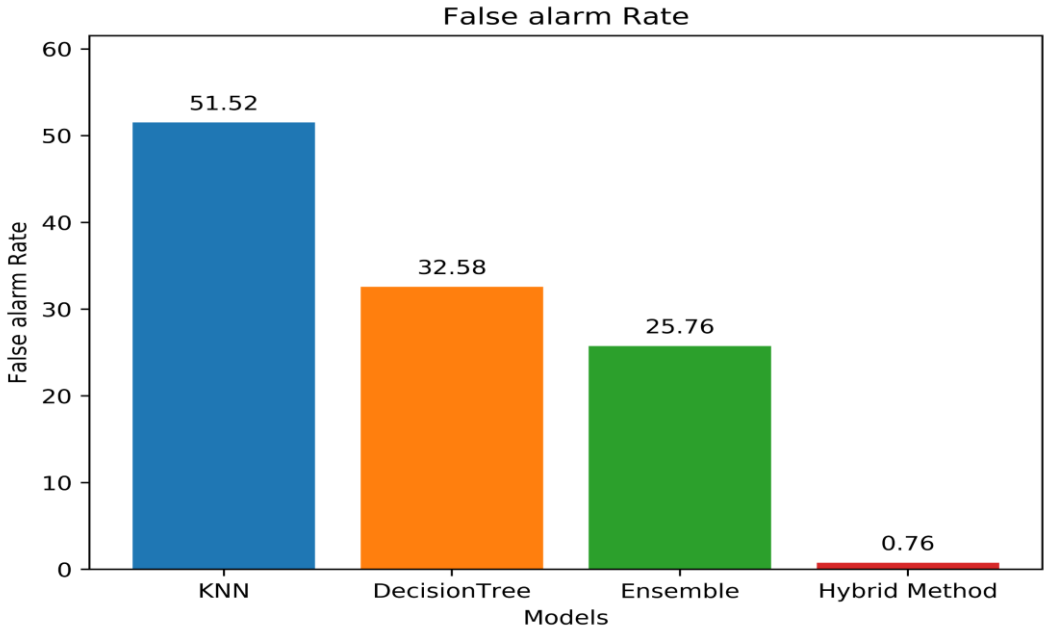

Figure 9 Comparative Analysis for False Alarm Rates

In ***Figure 9***, false alarm rates of four different ML models used for NIDS: KNN, DT, Ensemble, and a Hybrid Method. The KNN model shows the highest false alarm rate, indicating its limited reliability for scenarios where minimizing false positives is crucial. The Decision Tree model presents a significantly lower rate, suggesting a better but still imperfect performance. The Ensemble model further reduces the false alarm rate, demonstrating enhanced effectiveness through the combination of multiple model predictions.

Table 2 : Performance evaluation of KNN, DT, Ensemble Method and our hybrid method

Models	Accuracy	Precision	Recall	F-Measure	Detection Rate	False alarm Rate
KNN	48.48	55.26	72.58	40.63	48.48	51.52
DT	67.42	55.21	70.96	50.62	67.42	32.58
Ensemble Method	74.24	56.83	74.60	55.25	74.24	25.76
Proposed Hybrid Model	99.24	94.44	99.60	96.86	99.24	0.76

Table 2 shows the performance analysis of KNN, DT, Ensemble Method and our hybrid method. Remarkably, Our Hybrid Method outperforms all individual models, illustrating its superior accuracy and potential as a dependable solution in IDS.

5 Comparative Analysis of Existing State of Art

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

IDS in WSNs has become a crucial field of study. This analysis assesses various ML techniques designed to fortify the security of WSNs. One of the investigations presented a MK-ELM ML approach using Intrusion Detection in WSNs. This study focuses on not to compromise the performance of the network and the need for efficient security measures[35]. Another research enhanced accuracy by combining the SMOTE with RF to effectively tackle imbalances in the dataset [15].

Additionally, the OCIDS, which incorporates an advanced ABC optimization algorithm with a weighted SVM, displayed strong detection performance across benchmark datasets [16]. Further developments in intrusion detection include the use of various data mining techniques such as NB, Logistic Regression (LR), KNN, ANN and SVM. These methods have been applied to detect DoS attacks with high accuracy. A RF-based system, enhanced by the OMCFR method, achieved notable accuracy [17]. Additionally, the G-IDCS significantly minimized detection volume while improving accuracy [18]. A GAN optimized for the Industrial Internet of Things (IIoT) environments demonstrated superior detection rates [19]. An ELM, optimized with Enhanced Transient Search Arithmetic Optimization (ETSAO), also showed high efficacy in detecting anomalies [20].

Our work introduced a Hybrid ML model assessed on NSL-KDD dataset and achieved an improved 99.4% detection accuracy. False Alarm Rate is reduced to 0.76% which is significantly low compared to other existing methods. This demonstrates the model's superior performance and reliability in intrusion detection compared to existing state-of-the-art approaches [21]. **Table 3** shows the comparative study of proposed hybrid model with the existing methods.

Table 3 Comparison of Current Cutting-edge State of Art

Authors	Year	Algorithm	Dataset	Accuracy rate (%)
Tan Xiaopeng, et al. [15]	2019	Random Forest	WSN-DS	92.57
Shaimaa Ahmed Elsaid et al. [16]	2020	Support Vector Machine	NSL-KDD	97.90
Zhang et all. [35]	2020	MK-ELM	NSL-KDD	98.3%
Md Alauddin Rezvi et al. [17]	2021	Machine learning	WSN-DS	98.56
Shashank Gavel et al. [18]	2022	Random Forest	NSL-KDD	99.95
Sung Bum Park et al. [19]	2023	Graph-IDS	-	98.17

Received: August 07, 2025

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Irfan Ali Kandhro et al. [20]	2023	GAN	NSL-KDD	95-97
Chaya Ravindra et al.[21]	2023	Extreme Learning Machine	IBRL	97.4
Shalini Subramani et al.[28]	2023	PSO, Multiclass SVM	NSL-KDD19, KDD'99 Cup,CIDD	89.93%
U Nandhini et al.[23]	2024	Two stage classification using SVM and KNN	NSL-KDD	95.01%
Our Work	2024	Hybrid Method	NSL-KDD	99.24%

6 Conclusion & Future Scope

This study conducted a thorough comparative analysis of various ML models for NIDS in WSNs. The hybrid classification approach, which integrates multiple classifiers through a group decision mechanism, significantly outperforms individual classifiers in terms of accuracy, precision, recall, F-measure, detection rate, and false alarm rate. This strong framework emphasizes the effectiveness of ensemble methods and hybrid models in improving the security and dependability of network communications, providing a scalable option for real-time intrusion detection. The experimental results showed the hybrid model's ability to reach a high detection accuracy of 99.4%, positioning it as a viable option for practical implementation in WSN scenarios. This research adds valuable insights to the cybersecurity literature, shedding light on the advantages and challenges of various ML approaches for intrusion detection.

Future work should focus on integrating the hybrid intrusion detection model into real-time network systems by taking the energy efficiency as a factor. A trust factor can be assigned to nodes based upon the prediction provided by the hybrid model and can be considered in route management. This involves developing efficient data processing techniques to handle high-speed network traffic and ensuring that the IDS can operate with minimal latency and in energy efficient mode. By continuously updating the model with new data and retraining it periodically, the system can maintain high detection accuracy and adapt to new attack patterns. By addressing these future directions will enable researchers and practitioners to further enhance the capabilities of IDS. This will provide more robust and adaptive security solutions for protecting WSNs and other critical infrastructures from cyber threats.

7 Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

8 Data availability

Received: August 07, 2025

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

This study employed the NSL-KDD dataset. The dataset used for this study are available for download at https://github.com/HoaNP/NSL-KDD-DataSet. The code and other relevant data are available from the corresponding author on reasonable request.

9 Declaration of generative AI in scientific writing

The author(s) have not used any AI Content generation tool for writing this research article.

10 Third Party contributions

No person or third-party services were involved in the research or manuscript preparation beyond the listed authors.

11 List of Abbreviation

Table 4 List of Abbreviations

Abbreviation	Meaning
ABC	Artificial Bee Colony
ANN	Artificial Neural Network
AWID	Aegean Wi-Fi Intrusion Dataset
CAPSO	Chaos Adaptive Particle Swarm Optimization Algorithm
CNN	Convolutional Neural Network
DoS	Denial Of Service
DT	Decision Trees
ETSAO	Enhanced Transient Search Arithmetic Optimization
FPR	False Positive Rate
GAN	Generative Adversarial Networks
IBRL	Dataset Obtained From 54 Mica Sensors By The Intel Berkeley Research Lab
IDS	Intrusion Detection System
KNN	K-Nearest Neighbors
LR	Logistic Regression
ML	Machine Learning
NaN	Not A Number
NCA	Neighbourhood Component Analysis
NIDS	Network Intrusion Detection System
OCIDS	Optimized Collaborative Intrusion Detection System

Received: August 07, 2025

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

OMCFR	Optimized Maximum Correlation Based Feature Reduction
PSO	Particle Swarm Optimization
RF	Random Forest
RPL	Routing Protocol For Low-Power And Lossy Networks
SMOTE	Synthetic Minority Oversampling Technique
SVM	Support Vector Machine
URL	Uniform Resource Locator
WIDS	Wireless Intrusion Detection Systems
WLAN	Wireless Local Area Networks
WSN	Wireless Sensor Network

References

[1] J. Cecílio and P. Furtado, "Wireless Sensor Networks: Concepts and Components," 2014, pp. 5–25. doi: 10.1007/978-3-319-09280-5_2.

[2] N. D. Turg'unovna, "WIRELESS SENSOR NETWORK ARCHITECTURE AND CONTROL METHODS," *SCIENTIFIC ASPECTS AND TRENDS IN THE FIELD OF SCIENTIFIC RESEARCH*, vol. 2, no. 21, pp. 385–394, 2024.

[3] H. Sadia *et al.*, "Intrusion Detection System for Wireless Sensor Networks: A Machine Learning Based Approach," *IEEE Access*, vol. 12, pp. 52565–52582, 2024, doi: 10.1109/ACCESS.2024.3380014.

[4] S. Muneer, U. Farooq, A. Athar, M. Ahsan Raza, T. M. Ghazal, and S. Sakib, "A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis," *Journal of Engineering*, vol. 2024, pp. 1–16, Apr. 2024, doi: 10.1155/2024/3909173.

[5] Z. Chen, M. Simsek, B. Kantarci, M. Bagheri, and P. Djukic, "Machine learning-enabled hybrid intrusion detection system with host data transformation and an advanced two-stage classifier," *Computer Networks*, vol. 250, p. 110576, Aug. 2024, doi: 10.1016/j.comnet.2024.110576.

[6] H.-J. Liao, C.-H. Richard Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, Jan. 2013, doi: 10.1016/j.jnca.2012.09.004.

Received: August 07, 2025

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[7] S. Malathy *et al.*, "A review on energy management issues for future 5G and beyond network," *Wireless Networks*, vol. 27, no. 4, pp. 2691–2718, May 2021, doi: 10.1007/s11276-021-02616-z.

[8] R. Mitchell and I.-R. Chen, "A survey of intrusion detection in wireless network applications," *Comput Commun*, vol. 42, pp. 1–23, Apr. 2014, doi: 10.1016/j.comcom.2014.01.012.

[9] A. Heidari and M. A. Jabraeil Jamali, "Internet of Things intrusion detection systems: a comprehensive review and future directions," *Cluster Comput*, vol. 26, no. 6, pp. 3753–3780, Dec. 2023, doi: 10.1007/s10586-022-03776-z.

[10] A. Sezgin and A. Boyacı, "AID4I: An Intrusion Detection Framework for Industrial Internet of Things Using Automated Machine Learning," *Computers, Materials & Continua*, vol. 76, no. 2, pp. 2121–2143, 2023, doi: 10.32604/cmc.2023.040287.

[11] Md. A. Talukder *et al.*, "A dependable hybrid machine learning model for network intrusion detection," *Journal of Information Security and Applications*, vol. 72, p. 103405, Feb. 2023, doi: 10.1016/j.jisa.2022.103405.

[12] M. Adnan Khan, T. M. Ghazal, S.-W. Lee, and A. Rehman, "Data Fusion-Based Machine Learning Architecture for Intrusion Detection," *Computers, Materials & Continua*, vol. 70, no. 2, pp. 3399–3413, 2022, doi: 10.32604/cmc.2022.020173.

[13] Md. A. Talukder, Md. M. Islam, M. A. Uddin, A. Akhter, K. F. Hasan, and M. A. Moni, "Machine learning-based lung and colon cancer detection using deep feature extraction and ensemble learning," *Expert Syst Appl*, vol. 205, p. 117695, Nov. 2022, doi: 10.1016/j.eswa.2022.117695.

[14] D. Bianchi, N. Epicoco, M. Di Ferdinando, S. Di Gennaro, and P. Pepe, "Physics-Informed Neural Networks for Unmanned Aerial Vehicle System Estimation," *Drones*, vol. 8, no. 12, p. 716, Nov. 2024, doi: 10.3390/drones8120716.

[15] X. Tan *et al.*, "Wireless Sensor Networks Intrusion Detection Based on SMOTE and the Random Forest Algorithm," *Sensors*, vol. 19, no. 1, p. 203, Jan. 2019, doi: 10.3390/s19010203.

[16] S. A. Elsaid and N. S. Albatati, "An optimized collaborative intrusion detection system for wireless sensor networks," *Soft comput*, vol. 24, no. 16, pp. 12553–12567, Aug. 2020, doi: 10.1007/s00500-020-04695-0.

[17] M. A. Rezvi, S. Moontaha, K. A. Trisha, S. T. Cynthia, and S. Ripon, "Data mining approach to analyzing intrusion detection of wireless sensor

Received: August 07, 2025

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

network," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 1, pp. 516–523, 2021.

[18] S. Gavel, A. S. Raghuvanshi, and S. Tiwari, "An optimized maximum correlation based feature reduction scheme for intrusion detection in data networks," *Wireless Networks*, vol. 28, no. 6, pp. 2609–2624, 2022.

[19] S. B. Park, H. J. Jo, and D. H. Lee, "G-idcs: Graph-based intrusion detection and classification system for can protocol," *IEEE Access*, vol. 11, pp. 39213–39227, 2023.

[20] I. A. Kandhro *et al.*, "Detection of real-time malicious intrusions and attacks in IoT empowered cybersecurity infrastructures," *IEEE Access*, vol. 11, pp. 9136–9148, 2023.

[21] C. Ravindra, M. R. Kounte, G. S. Lakshmaiah, and V. N. Prasad, "Etelmad: anomaly detection using enhanced transient extreme machine learning system in wireless sensor networks," *Wirel Pers Commun*, vol. 130, no. 1, pp. 21–41, 2023.

[22] P. Nancy, S. Muthurajkumar, S. Ganapathy, S. V. N. Santhosh Kumar, M. Selvi, and K. Arputharaj, "Intrusion detection using dynamic feature selection and fuzzy temporal decision tree classification for wireless sensor networks," *IET Communications*, vol. 14, no. 5, pp. 888–895, Mar. 2020, doi: 10.1049/iet-com.2019.0172.

[23] U. Nandhini and S. K. SVN, "An improved Harris Hawks optimizer based feature selection technique with effective two-staged classifier for network intrusion detection system," *Peer Peer Netw Appl*, Sep. 2024, doi: 10.1007/s12083-024-01727-6.

[24] H. Bangali *et al.*, "Prediction of middle box-based attacks in Internet of Healthcare Things using ranking subsets and convolutional neural network," *Wireless Networks*, vol. 30, no. 3, pp. 1493–1511, Apr. 2024, doi: 10.1007/s11276-023-03603-2.

[25] K. Yesodha, M. Krishnamurthy, M. Selvi, and A. Kannan, "Intrusion detection system extended CNN and artificial bee colony optimization in wireless sensor networks," *Peer Peer Netw Appl*, vol. 17, no. 3, pp. 1237–1262, May 2024, doi: 10.1007/s12083-024-01650-w.

[26] A. Kannan, M. Selvi, S. V. N. Santhosh Kumar, K. Thangaramya, and S. Shalini, "Machine Learning Based Intelligent RPL Attack Detection System for IoT Networks," 2024, pp. 241–256. doi: 10.1007/978-981-99-9718-3_10.

[27] S. Subramani, M. Selvi, S. V. N. S. Kumar, K. Thangaramya, M. Anand, and A. Kannan, "An Intrusion Detection System for Securing IoT Based Sensor

Volume 38 No. 4s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Networks from Routing Attacks," 2023, pp. 321–334. doi: 10.1007/978-3-031-39811-7_26.

[28] S. Subramani and M. Selvi, "Multi-objective PSO based feature selection for intrusion detection in IoT based wireless sensor networks," *Optik (Stuttg)*, vol. 273, p. 170419, Feb. 2023, doi: 10.1016/j.ijleo.2022.170419.

[29] S. Rajasoundaran, S. V. N. S. Kumar, M. Selvi, K. Thangaramya, and K. Arputharaj, "Secure and optimized intrusion detection scheme using LSTM-MAC principles for underwater wireless sensor networks," *Wireless Networks*, vol. 30, no. 1, pp. 209–231, Jan. 2024, doi: 10.1007/s11276-023-03470-x.

[30] Y. Duan, N. Chen, L. Chang, Y. Ni, S. V. N. S. Kumar, and P. Zhang, "CAPSO: Chaos Adaptive Particle Swarm Optimization Algorithm," *IEEE Access*, vol. 10, pp. 29393–29405, 2022, doi: 10.1109/ACCESS.2022.3158666.

[31] A. B. Abhale and S. S. Manivannan, "Supervised machine learning classification algorithmic approach for finding anomaly type of intrusion detection in wireless sensor network," *Optical Memory and Neural Networks*, vol. 29, no. 3, pp. 244–256, 2020.

[32] S. Otoum, B. Kantarci, and H. T. Mouftah, "A novel ensemble method for advanced intrusion detection in wireless sensor networks," in *Icc 2020-2020 ieee international conference on communications (icc)*, IEEE, 2020, pp. 1–6.

[33] D. Wang and X. Tan, "Bayesian neighborhood component analysis," *IEEE Trans Neural Netw Learn Syst*, vol. 29, no. 7, pp. 3140–3151, 2017.

[34] W. Li, P. Yi, Y. Wu, L. Pan, and J. Li, "A new intrusion detection system based on KNN classification algorithm in wireless sensor network," *Journal of Electrical and Computer Engineering*, vol. 2014, no. 1, p. 240217, 2014.

[35] W. Zhang, D. Han, K. C. Li, and F. I. Massetto, "Wireless sensor network intrusion detection system based on MK-ELM," *Soft comput*, vol. 24, no. 16, pp. 12361–12374, Aug. 2020, doi: 10.1007/s00500-020-04678-1.

Received: August 07, 2025