

Available online at [www.qu.edu.iq/journalcm](http://www.qu.edu.iq/journalcm)

JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS

ISSN:2521-3504(online) ISSN:2074-0204(print)



# Energy-Aware Hybrid AI Framework for Intelligent Threat and Anomaly Detection in Resource-Constrained Wireless Sensor Networks

Raghad Tariq AL\_Hassani<sup>a</sup>, Zainab Ali Abbood<sup>b</sup>, Adil M. Salman<sup>c</sup>

<sup>a</sup>Ministry of Higher Education and Scientific Research, Minister's Office, Baghdad, Iraq. [eng\\_raghadtarik@yahoo.com](mailto:eng_raghadtarik@yahoo.com):

<sup>b</sup>Computer Technology Engineering Department, Al-Mansour University College, Baghdad, Iraq. [zainab.a.abbood@muc.edu.iq](mailto:zainab.a.abbood@muc.edu.iq) :

<sup>c</sup>Cybersecurity Engineering Department, Al-Iraqia Science University, Baghdad, Iraq. [adelmsk63@baghdadcollege.edu.iq](mailto:adelmsk63@baghdadcollege.edu.iq) :

## ARTICLE INFO

### Article history:

Received: 20 /04/2026

Rrevised form: 03 /05/2026

Accepted : 05 /05/2026

Available online: 30 /09/2026

### Keywords:

Artificial Intelligence (AI),

Wireless Sensor Networks (WSNs);

Energy-Aware Security;

Anomaly Detection;

Convolutional Neural Networks (CNN);

Random Forest (RF).

## ABSTRACT

This paper presents an energy aware hybrid Artificial Intelligence (AI) approach to intelligent threat detection and anomaly identification in resource restricted Wireless Sensor Networks (WSNs). However, securing the computer systems remains one of the challenging issues due to limited energy resources, computational capacity, and dynamic characteristics of WSN nodes. To overcome all of the above problems, this paper introduces a hybrid framework that combines Convolutional Neural Networks (CNN) and Random Forest (RF) algorithms to enable accurate and efficient detection of multiple cyber threats such as Distributed Denial of Service (DDoS) attacks, malware intrusions, data breaches, unauthorized access attempts and more. Furthermore, an adaptive anomaly detection method is designed to learn from network traffic and sensor data in order to detect abnormal patterns that may reflect security vulnerabilities. The proposed model adopts an energy-awareness approach, unlike traditional approaches; minimizing computational efforts while achieving high detection performance that is suitable for WSN environments with resource constraints. The results of our exploration show that the hybrid CNN+RF model provides high accuracy for threat classification and uniquely detects anomalies in real-time approaches. The proposed study shows a greener way of providing lightweight energy efficient intelligent detection for an anomalous event using modern techniques in WSN by means of deep learning and machine learning approaches. thus, this gives rise to better threat discovery and detection at earliest stages which in turn, helps in enhanced functionality from a security point of view all over WSN.

<https://doi.org/10.29304/jqcm.2026.18.32828>

## 1. Introduction

The recent years have seen the quick progress of IoT technologies and smart sensing applications, fostering thousands of wireless sensor networks (WSNs) that are at the heart for many fields such as environmental monitoring [1], healthcare systems [2], industrial automation systems [3] and smart cities. According to [4], WSNs consist of a large

\*Corresponding author

Email addresses: [eng\\_raghadtarik@yahoo.com](mailto:eng_raghadtarik@yahoo.com)

Communicated by 'sub etitor'

number of sensors which communicate without centralized infrastructures. WSNs monitor physical or environmental conditions, and often cooperate. Although their flexibility and scalability are an advantage, WSNs are often limited in terms of energy resources, current computing power and memory [5,6], making them subject to different cyber-security vulnerabilities.

WSNs handle sensitive information and are vulnerable to advanced cyber-attacks DDoS, malware attack, data corruption, unauthorized access attempts [7,8], so ensuring their security is a critical challenge. Traditional prevention systems, whether a classical intrusion detection system or even some simple rule-based methods, in WSN environments are too sophisticated due to their computational complexity expression and lack of adaptation ability leading to static preventive reaction they define; hence these approaches do not work under dynamic and resource authority [9]. Furthermore, the limited energy capacity of sensor nodes requires lightweight and effective security methods.

Thus, to counter these problems in the recent years research has focused on AI techniques such as machine learning and deep learning methods to strengthen threat detection and anomaly identification process within WSNs. More recently, AI-based approaches have demonstrated a strong capability to identify advanced patterns of attacks and adjust to an expanding variety of threats with high detection performance [10]. However, the majority of previous proposals discussed different domains but did not adequately address energy efficiency and computational optimization techniques as these play a significant role in WSN domains.

In this paper, the hybrid AI framework is introduced for energy Aware intelligent threat detection and anomaly detection in resource constrained WSNs includes CNN and RF algorithms. In this work we propose a framework that can analyze network data along with sensor data to identify anomalous behavior indicative of security events. In addition, the model achieves high detection performance with low computation complexity and energy consumption. The main contributions of this work can be summarized as follows:

1. Development of a hybrid AI-based framework combining CNN and RF for enhanced threat detection in WSNs.
2. Design of an energy-aware mechanism to ensure efficient operation in resource-constrained environments.
3. Implementation of an anomaly detection model capable of identifying abnormal patterns in both sensor data and network traffic.
4. Comprehensive evaluation demonstrating improved detection accuracy and efficiency compared to traditional methods. The challenges associated with cybersecurity in WSNs are illustrated in Fig 1.

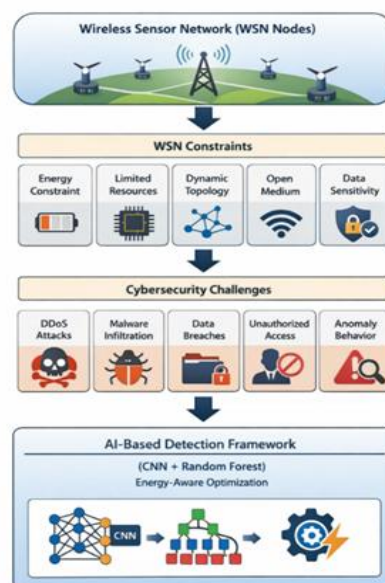


Fig. 1 - cybersecurity challenges in WSN.

The paper is structured as follows. Section 2 reviews related work about WSN cybersecurity and AI-enabled detection methods. The section 3 elaborates the proposed methodology, followed by the design of CNN–RF hybrid model and energy-aware optimization strategy. This is followed by Section 4, which shows the experimental results and performance. Section 5 concludes the paper and discusses the future work.

## **2. Related Work**

The technological development of WSNs has increased their usage in scientific areas [8], and this has brought several applications in important sectors such as environmental monitoring, health systems, industry automation, smart structures [9–11]. Nevertheless, the special features of WSNs such as limited energy resources, limited computing power and distributed architectural have posed significant challenges for cybersecurity [12,13]. Consequently, extensive research work has been on designing effective and lightweight security mechanisms specifically for WSN environment.

WSNs are automatically vulnerable to cyber-attacks, and as a result, there has been great discussion on using IDS as the first line of defense against threats [14,15]. Conventional network-based IDS approaches involve centralized architectures with high computational resources, which are not suitable for resource-constrained WSNs [16]. To address these limitations, researchers have proposed distributed and lightweight IDS models that can work efficiently within sensor networks [17].

Many research works have addressed the problem using supervised machine learning algorithms like DT, SVM and RF in IDS frameworks to classify network traffic as normal or malicious [18,19]. In particular, RF is widely recognized for its robustness as well as high accuracy in dealing with complex datasets with low overfitting [20]. A fundamental drawback of these methods is that they do not take into account energy consumption, which continues to be an important problem in WSNs.

Anomaly detection techniques are important characteristics to recognize unknown and new cyclone assaults in WSNs [21] due to evolving threat. In contrast to the signature-based method, anomaly detection does not depend on pre-specified patterns and detects anomalies in sequence of packets when it deviates from normal network behavior, thus it is more useful against zero-day attacks [22].

Over the last few years, deep learning models, especially CNNs, have also been used for abnormal behaviour detection in network traffic analysis [23]. CNNs can learn high-level features from complex datasets, which leads to better detection accuracy than traditional machine learning methods [24]. The efficiency of CNN-based models in identifying DDoS attacks, malware activities, and anomalies in WSN communication has been established by a number of studies [25,26].

However, the majority of already existing anomaly detection frameworks fail to incorporate such hybrid approaches that combine deep learning models with traditional machine learning ones. Additionally, little consideration has been given to achieving energy-efficient models which are vital for maintaining sustainability in the environments of WSN [27]. There has also been a significant amount of work done on secure routing protocols to defend WSN from several network-layer attacks such as black hole, wormhole, Sybil and selective forwarding attacks [28,29]. Its defined protocols will ensure secure data transmission between sensor nodes with least effect of malicious nodes.

To ensure routing security, several approaches utilize cryptographic technique and trust-based mechanism [30]. However, these strategies can lead to higher computational overhead and energy consumption [31], leading to a decrease in the network performance. As a result, the demand for smart and adaptive security solutions that can juggle security needs against resource limitations is increasing.

Despite the remarkable advancements in leveraging AI approaches on WSN security, many serious challenges facing this topic are still not addressed. First, many of the existing solutions depend on either machine learning or deep learning models without considering the complementary strengths of these hybrid approaches [32]. Second, most existing frameworks do not take the energy-awareness into consideration as a main requirement for resource-limited WSN environments [33]. Third, relatively few works have proposed a method which combines both network traffic and sensor data for real-time anomaly detection [34,35].

Thus, categorizing the attacks based on their behavior and effect on the network operation is quite essential towards realizing the variety of security threats in WSNs. The resource constraints in WSNs such as low energy resources, broadcast communications and/or distributed architecture take advantage of an increasing number of various attacks targeted at different layers of the network. The categorized means provides a precise view for the learning of likely

including detection and avoidance strategies in WSNs. Building effective AI-powered intrusion detection and anomaly detection systems require knowledge of the characteristics of each malware attack type. The taxonomy of classical cyber-attack concerning the WSN environment, their description, and impact on network security is detailed in Table 1.

**Table 1: Taxonomy of Cyber Attacks in Wireless Sensor Networks and Their Impact on Network Security**

| Category of Attack             | Type of Attack                         | Description in WSN Context                                                                                             | Reference  |
|--------------------------------|----------------------------------------|------------------------------------------------------------------------------------------------------------------------|------------|
| <b>Probe Attacks</b>           | Port Scanning, Network Mapping         | Attackers gather information about network topology, node IDs, and communication patterns to identify vulnerable nodes | [14], [18] |
| <b>Denial-of-Service (DoS)</b> | Flooding, Jamming, Exhaustion          | Attackers overwhelm sensor nodes or communication channels, causing energy depletion and service disruption            | [21], [25] |
| <b>Remote-to-Local (R2L)</b>   | Unauthorized Access, Password Guessing | External attackers gain access to sensor nodes or base stations without proper authentication                          | [19], [26] |
| <b>User-to-Root (U2R)</b>      | Privilege Escalation, Rootkits         | Attackers obtain higher privileges to control network operations and manipulate system behavior                        | [20], [27] |
| <b>Routing Attacks</b>         | Black Hole, Wormhole, Sybil            | Malicious nodes manipulate routing paths to drop, alter, or redirect packets within the network                        | [28], [29] |
| <b>Data Integrity Attacks</b>  | Data Injection, Data Modification      | Attackers alter sensor readings or inject false data, affecting decision-making processes                              | [30], [31] |
| <b>Anomaly-Based Attacks</b>   | Zero-day Attacks, Unknown Behavior     | Attacks that deviate from normal patterns and are difficult to detect using signature-based methods                    | [22], [34] |

To overcome these limitations, in this research an energy-aware hybrid AI framework combining CNN and RF algorithms has been proposed. The method is expected to deliver high detection accuracy along with both computational efficiency and low energy consumption, thus offering a viable and scalable cybersecurity solution for WSNs.

### 3. Methodology

This proposed method for smart threat detection and anomaly detection combines the properties of CNN & RF models with resource restrictions imposed via WSN. It is a step-by-step approach starting from the network model, data generation, attack simulation and goes on to model training and evaluation as well as performance analysis.

#### 3.1. Design

##### 3.1.1. Explanation of Approach

This section describes building and evaluation of AI-based intrusion detection and prevention system in a simulated WSN environment. However, WSNs have limited battery capacity and computational resources, which necessitates lightweight and energy-efficient solutions. In a controlled environment, the simulation generates normal user behavior and malicious activities DDoS attacks using realistic sensor data and network traffic patterns. Currently, a RF classification model based on CNN high-order diagrams is proposed.

The sensor data generation and traffic generation follow the WSN model construction, after which attack simulation is conducted. Then, a hybrid AI model mixing CNN and RF is trained and evaluated to determine its performance. In

Table 2, we summarize our experimental design the procedure goes from network modeling and data generation to model training/evaluation and overall performance evaluation in WSN environment.

**Table 2: Experimental Setup for AI-Based IDPS in Simulated WSN Environment**

| Experiment Stage                    | Description                                                                                                                        |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| WSN Model Creation                  | Develop a simulated WSN environment with multiple sensor nodes, considering energy constraints and communication patterns          |
| Data Generation & Attack Simulation | Generate normal sensor data and simulate cyber-attacks such as DDoS, data injection, and unauthorized access                       |
| Model Training                      | Train CNN for feature extraction and RF for classification using labeled datasets                                                  |
| Model Evaluation                    | Evaluate model performance using accuracy, precision, recall, and F1-score                                                         |
| Performance Assessment              | Analyze system efficiency in terms of detection accuracy, energy consumption, real-time response, and anomaly detection capability |

### 3.1.2. Explanation of Selected Method

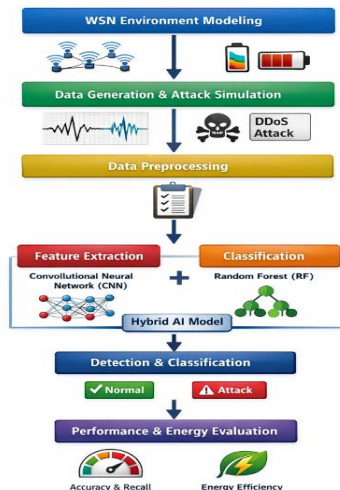
In this paper, we present an initial investigation of the detection and response capacity of this novel approach under controlled conditions. This allows reproducibility, performance comparison, and validation of the proposed framework to make claims regarding its ability in detecting cyber threats on WSN environments. It also enables the navigation of the accuracy versus energy efficiency trade-off in detection rate.

### 3.1.3. WSN Modeling, Attack Simulation, and AI-Based IDPS Implementation

To evaluate our proposed scheme, we implemented a simulated WSN to contain numerous energy-constrained sensor nodes. Thus, the network traffic and sensor readings generated under this framework mimic normal operational behavior. Then, different cyber-attacks are simulated:

- 1 Distributed Denial of Service (DDoS)
- 2 Data injection attacks
- 3 Unauthorized access attempts

The dataset is preprocessed and split into training and testing sets. A CNN model is trained to automatically capture the deep features, while a Random Forest classifier is used to classify normal or malicious network behavior. Furthermore, the suggested framework comprises of lightweight computation mechanisms to decrease processing overhead on sensor nodes in order to ensure energy efficiency. In this section, a flowchart of the proposed methodology is shown in fig. 2, where it contains the steps of data generation followed by different model training stages and its performance evaluation.



**Fig. 2 - flowchart of the proposed energy-aware hybrid AI-based intrusion detection and anomaly detection framework in WSNs.**

### 3.2. Data Collection

The following section details the data collection method used to train and test the proposed energy-aware artificial intelligence-based IDPS in a simulated WSN scenario. Hence, taking into account the resource and energy constraints for WSN nodes will allow to capture both normal and malicious network behavior. The process comprises three steps: WSN model generation, data generation, and cyber-attack simulation.

#### 3.2.1. WSN Network Model Creation Process

Our proposed WSN model captures some of the main sensor networks features: lack of energy resources, limited computation power, and distributed communication between sensors. The model includes:

1. Random deployment of sensor nodes in a predetermined area of interest
2. Description of Communication Between Node and Base Station (sink node)
3. The network parameters configuration like transmission range, sensing range and energy levels of the nodes
4. Usage of static or semi-static nodes i.e. fixed in nature (common for WSNs). This configuration allows realistic simulation of WSN behavior and communication.

#### 3.2.2. Data Generation Process for the WSN Network

After the WSN model has been created, synthetic data to emulate sensor readings and network traffic behaviour is produced. The dataset includes:

1. Sensor data (e.g., temperature, humidity and so on environmental readings);
2. Sensor nodes packet transmission logs
3. Schemes of communications and action plan
4. Energy consumption at the nodes for data transmission and processing. These data show normal network behavior and serve as a baseline for anomaly detection.

#### 3.2.3. Simulation of Cyber Attacks in WSN

Indeed, the WSN environment is created by simulating several Cyber-attacks in order to measure the effectiveness of all features proposed by the IDPS. These include:

- 1 **DDoS:** Overwhelming sensor nodes with too much traffic to use up energy resources
- 2 **Data Injection Attacks:** Injecting false sensor readings into the network
- 3 **Unauthorized Access:** Mimicking malicious nodes trying to enter network resources

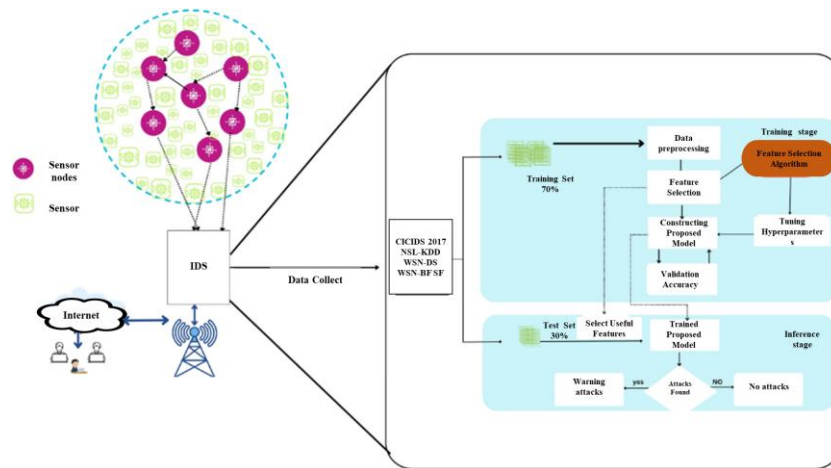
Attack scenarios can produce labeled datasets that behave normally or maliciously, and these are critical for training AI models.

#### 3.2.4. Dataset Objective

this reason, the data collection process is designed to yield a complete dataset covering: Normal WSN operations, Abnormal and attack scenarios and Energy consumption that serve as the baseline for training and evaluating the hybrid CNN-RF model for intelligent threat detection and anomaly identification.

As depicted in this diagram, the overall workflow of our proposed energy-aware AI-based IDPS is shown as a complete frame. The process begins with data collection in WSN, followed by data preprocessing, feature selection, and model

training using Artificial Intelligence techniques like CNN and RF. As well, it provides info. on splitting up the data into a training & testing phase. Fig.3 presents the architecture and data processing pipeline of an implemented AI based IDPS framework.



**Fig. 3 - data collection process for the proposed energy-aware AI-based IDPS in WSNs, including network modeling, data generation, and attack simulation.**

Table 3 Summary of parameters for simulation configuration of WSN in this work The parameters are selected to capture realistic WSNs and particularly the energy constraints and communication behavior. This allows you to explore the behavior of the proposed AI-based IDPS within a multitude of operational and attack scenarios with high accuracy.

**Table 3: WSN Network Parameters**

| Parameter              | Description                               |
|------------------------|-------------------------------------------|
| Number of Nodes        | 50 sensor nodes                           |
| Network Type           | Distributed WSN with sink node            |
| Transmission Range     | 50-100 meters                             |
| Node Deployment        | Random deployment                         |
| Mobility Pattern       | Static or low mobility                    |
| Communication Protocol | LEACH / Energy-efficient routing protocol |
| Initial Energy         | 0.5 – 2 Joules per node                   |
| Sensing Area           | 100 × 100 m <sup>2</sup>                  |

### 3.3. Preparation of Data

In the data-collection phase, the gathered dataset is pre-processed to be able to train and evaluation of the proposed energy-aware AI-based IDPS in a simulated environment for WSN. In resource-constrained WSN scenarios, data preparation is an essential step prior to dataset creation in order to guarantee quality, consistency and effectiveness. The two main steps in the data preparation are splitting and preprocessing. To reduce the risk of overfitting and ensure model generalization, k-fold cross-validation (k=5) is used. This allows the model to be tested on different parts of the data, improving the model's accuracy and stability.

### 3.3.1. Data Splitting for AI-Based IDPS Model

We used the retrieved dataset split into a training and test set. The data presented for this analysis is also split into two, one to be used in training the hybrid AI model (CNN + RF) and is testing on the out samples as to how well it was able to detect cyber threats and anomalies. The standard Train-Test split ratio was 70–30 to achieve balanced evaluation. It may also perform cross-validation technique for better generality of model and reduction in overfitting. This guarantees evaluation of the proposed model on unseen data, thus enabling realistic representation of the model's efficacy in WSN scenarios.

To properly prepare the dataset for training the proposed energy-aware AI-based IDPS, important steps are performed in the data preparation phase. This requires splitting the dataset and applying many of the preprocessing steps to make the data clean, effective for model learning/accuracy, and guarantee reliable detection in resource-constrained Wireless Sensor Networks (WSN). Table 4 lists issues of data cleaning and their goal.

**Table 4: Structured Data Preparation Workflow for Energy-Aware AI-Based IDPS in WSNs**

| Stage                          | Process                     | Description                                                                                       | Purpose                                             |
|--------------------------------|-----------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| <b>Data Splitting</b>          | Training & Testing Division | The dataset is divided into training (70%) and testing (30%) sets, with optional cross-validation | Ensure unbiased model evaluation and generalization |
| <b>Preprocessing</b>           | Data Normalization          | Scale numerical features such as sensor readings and traffic attributes                           | Improve model convergence and stability             |
| <b>Preprocessing</b>           | Feature Engineering         | Extract features such as packet rate, communication frequency, and energy consumption             | Enhance detection of normal and malicious patterns  |
| <b>Preprocessing</b>           | Missing Value Handling      | Apply imputation techniques to fill missing data                                                  | Maintain dataset consistency                        |
| <b>Preprocessing</b>           | Categorical Encoding        | Convert categorical variables into numerical form                                                 | Enable compatibility with AI models                 |
| <b>Preprocessing</b>           | Data Balancing              | Apply oversampling or undersampling techniques                                                    | Prevent bias toward dominant classes                |
| <b>Energy-Aware Processing</b> | Energy Feature Integration  | Include residual energy and energy consumption metrics                                            | Improve energy-efficient threat detection           |

### 3.4. AI Algorithms Training

The CNN and RF refer to the two AI models being trained, which are described in this section. In the training of these models, prepared dataset is used to develop effective IDPS for detecting and preventing cyber-attacks in simulated environment of WSN.

As a suggested framework, a hybrid model is proposed which requires CNN to extract deep features from both sensor data and the network traffic separately while RF is used for classification of normal and malicious activities. This enables a better performance in detection at all levels of accuracy while considering the computational efficiency, which is one of the major factors to take into account for WSNs with limited resources.

The trained models are evaluated using the common metrics accuracy, recall, precision and F-measure (F1-score). These are the above metrics showing a complete analysis of how well CNN and RF models have worked in identifying cyber threats ANOMALIES against dataflow within WSN network. This is the overall correctness of the model and it

is calculated as Correctly Predicted instances / Total Number of Instances. The accuracy rate shows how well the model is able to classify whether a given network traffic behavior is normal or malicious. (See Eq. 1).

$$\text{Accuracy (ACC)} = \frac{TP+TN}{FP+FN+TP+TN} \quad (1)$$

Recall (also known as sensitivity or true positive rate) measures the ability of a model to find positive instances (in our case malicious network behavior) out of all actual positive instances. It is defined as the proportion of positives that were correctly identified, made up of true positives and false negatives. (See Eq. 2).

$$\text{Recall: } \frac{TP}{TP+FN} \quad (2)$$

Precision is the fraction of positive instances that were correctly predicted by the model, and is defined as  $TP/(TP + FP)$ . The number of malicious actually predicts positive instances. (See Eq. 3).

$$\text{Precision} = \frac{TP}{TP+FP} \quad (3)$$

The F-measure, or the F1-score, is the harmonic mean of precision and recall. It gives a balanced measure of both false positives and false negatives. Higher F1 scores reflect better overall model performance. (See Eq. 4).

$$F - \text{measure (F1)} = \frac{2 * \text{PRECISION} * \text{RECALL}}{\text{PRECISION} + \text{RECALL}} \quad (4)$$

### 3.4.1. Training for CNN Model

Thus, this subsection further clarifies that how a CNN model is trained to accurately recognize and combat IDPS in a simulated WSN environment by optimizing its architecture as well as hyperparameters. This dynamic architecture has enough capacity to extract features from the sensor data and network traffic for classification with small models constrained for WSN nodes. The following are the main steps of training:

1. **Initialization:** The architecture of the CNN needs to be defined which includes setting up the number and type of layers such as convolutional layer, pooling layer, fully connected layers and selecting an appropriate activation function. WSN limitations drove the architecture to balance feature extraction capability and computational efficiency.
2. **Compile:** In this phase defines the loss function, optimizer and evaluation criteria. This enables to set the rules for how updates are made in model parameters during training. Activation functions are selected to reduce computation overload and energy consumption.
3. **Training:** CNN model is trained over the prepared dataset that consists of both normal and malicious behavior. In this approach, the model learns by iteratively updating its weights and biases using input data to improve its performance on classifying network behavior for cyber threats in WSN environments.
4. **Validation:** The model is validated on a different dataset to check performance and for stopping overfitting. This enables the model to generalize well to unseen data and maintain accurate detection performance.
5. **Fine-Tuning:** The hyperparameters like learning rate, number of filters and batch size are optional fine-tuned to achieve better results. This process improves the model performance to identify anomalies and attacks while ensuring that the WSNs operate in an energy-efficient manner

For the sake of reproducibility and to give an implementation detail, the CNN architecture is described here. It comprises three convolutional layers with 32, 64 and 128 filters respectively, kernel size  $3 \times 3$ , and ReLU activation. Each convolutional layer is followed by a max-pooling layer with a pool size of  $2 \times 2$ . The dense layer has 128 neurons and a Softmax layer as the output. The CNN is trained with the Adam optimizer, a learning rate of 0.001 and the loss is calculated by using categorical cross-entropy. The batch size is 32 with 50 epochs of training. A diagram is presented to illustrate the training workflow of the proposed CNN model which provides a clear perception on its training process. This emphasizes the stepwise process of initializing, compiling, training, validating and finally fine-tuning models. Furthermore, it is indicative of the optimization of the model aimed at efficiently learning feature representations from sensor data as well as network traffic while conserving energy within resource-constrained

WSN environments. The training process of the CNN model applied in the proposed AI-based IDPS framework is shown in Fig.4.



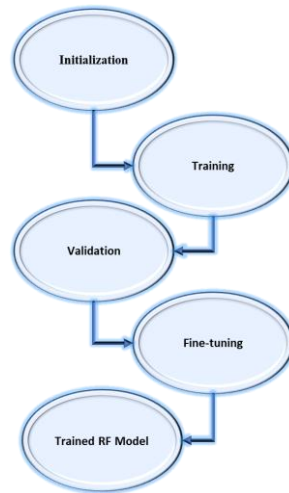
**Fig. 4 - Training process of the CNN model for energy-aware intrusion detection and anomaly detection in WSNs.**

### 3.4.2. Training for RF Model

The training process of RF model, an ensemble learning algorithm used for a tactical data and IDPS tasks in a simulated WSN, is described in this subsection. The RF model is very well suited for WSNs due to their robustness, low computational complexity, and effectiveness in dealing with high dimensional data. The training process includes:

- 1 **Initialization:** important hyperparameters: number of decision trees to create, maximum tree depth, and the criterion for splitting nodes (e.g. Gini index or entropy) These metrics are chosen at the cost of classification performance and computation time since such parameters play significant role in WSN with limited resources.
- 2 **Training:** The RF model is trained on the prepared dataset, where multiple decision trees are built using random data and features of training. This allows the ensemble approach to achieve high accuracy in the classification task while avoiding overfitting, making it possible to identify various types of cyber-attacks in and through WSN traffic and data from individual sensors.
- 3 **Validation:** trained model is evaluated via a separate validation dataset to evaluate its simplification capability. This step ensures that the model can accurately classify unseen data and maintain reliable performance in real-world WSN situations.
- 4 **Fine-Tuning:** This optional phase involves tuning hyperparameters in order to further fit the model. We optimize parameters like the number of trees, feature selection strategy, and tree depth for increased accuracy in detection with power-efficient operation.

The Random Forest model uses 100 trees to provide accurate classification. A maximum tree depth of 10 is chosen to avoid overfitting, and the Gini index is used for splitting. The model automatically selects features at each node using random feature subsets. These settings are chosen to achieve a trade-off between classification accuracy and computational resources in WSN settings. Structure of train RF model for representation work flow How many decision trees are created, modified and performed to give stable classification performance This means that the model's performance is optimized for executing WSN in a resource-constrained basis and risk detection. The flow chart of training the Random Forest Model in proposed Framework of AI-based IDPS is shown in Fig. 5.



**Fig. 5 - Training process of RF model for energy-aware intrusion detection and anomaly detection in WSNs.**

### 3.5. IDPS Evaluation

This section presents the evaluation of the proposed IDPS solution in WSN simulated environment. The assessment and evaluation of the considered data-driven approach are beyond key performance indicators such as detection of attack, detection of anomaly, real-time response, resource efficiency and privacy conservation rather ensure that there are secure and reliable operations to a constrained resource WSNs. CNN and Random Forest modeling based proposed system gives the performance that is evaluated by commonly used evaluation parameters of accuracy, true positive rate as well as false positive rate. Likewise, the system capability to identify abnormal events, respond immediately, perform with limited resources and ensure privacy is studied in order to demonstrate utility of the system in practical WSN scenarios. Which provides a summarized sketch of comprehensive assessments framework for evaluation matrix on desirable IDPS. They represent the ability to accurately identify cyberattacks, inability to diagnose abnormal behaviour and then investigate the system that corresponds correctly in real-time for effective performance under resource restrictions with data privacy in a WSN context. Table 5 provides an elaborate description of the assessment features and their significance in WSN based cyber security systems with this information.

**Table 5: Evaluation Metrics of the Proposed IDPS**

| Evaluation Aspect          | Description                                                                                                                                                         | Importance in WSN                                               |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| <b>Attack Detection</b>    | Evaluates the system's ability to accurately classify network traffic using metrics such as Accuracy (ACC), True Positive Rate (TPR), and False Positive Rate (FPR) | Ensures reliable identification of cyber threats                |
| <b>Anomaly Detection</b>   | Identifies abnormal patterns and deviations from normal network behavior                                                                                            | Enables detection of unknown and zero-day attacks               |
| <b>Real-Time Response</b>  | Measures the system's ability to detect and respond to attacks in real time                                                                                         | Minimizes the impact of attacks and ensures network stability   |
| <b>Resource Efficiency</b> | Assesses computational cost, memory usage, and energy consumption of the system                                                                                     | Critical for operation in resource-constrained WSN environments |

|                             |                                                                                     |                                                                         |
|-----------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| <b>Privacy Preservation</b> | Ensures secure handling and protection of sensitive data during detection processes | Maintains data confidentiality and compliance with privacy requirements |
|-----------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------|

To demonstrate the performance of the proposed hybrid CNN-RF model, a comparison is made with conventional machine learning models, such as Support Vector Machine (SVM) and Decision Tree (DT). The findings show that the hybrid CNN-RF model has better performance in terms of detection and anomaly recognition.

## 4. Results and Discussion

In this section, the performance analysis of the proposed IDPS is presented through the simulation results from a WSN network. It is aimed at calculating and recording the performance of AI-based CNN, RF cyber threat detection and mitigation systems. It looks at a wider scope of parameters such as metrics for assessing model performance, the directional capacity to identify attacks and aberrations, real-time responsiveness, resource deployment and privacy upholding. These modules are important to evaluate the strength and the potential deployment avenues of their proposed solution in resource-constrained WSN environments. Finally, here you will be able to discuss the importance of obtained results, advantages of suggested framework and what is required in next generation AI based IDS.

### 4.1. AI Models Performance Evaluation

This section provides a detailed evaluation of the performance of two AI models, namely CNN and RF, in detecting cyber-attacks within the simulated WSN environment.

#### 4.1.1. CNN Evaluation Performance

To evaluate the performance of CNN model, different evaluation metrics are used such as accuracy in addition to recall, precision and F1-score. The result demonstrates that with CNN model, the accuracy can reach 75% and thus a big portion of network traffic samples in WSN environments are classified accurately by the proposed method. We were able to measure a recall value of 60%, tool recognized real attack events and that it is somewhat sensitive to malicious activities. In addition, with an accuracy score of 80%, this indicates that the model has a low false positive prediction as most of all detected attacks are true malware. F1-score 68% is a great metric as it takes in to account precision along with recall.

Hence, in response to the above-mentioned problem, CNN model performs well when detecting cyber threats on WSN. This recall, despite being much lower than precision, shows that some attack instances can still go undetected and it calls for further optimization and improvement. In order to make clearer the results performance from CNN model, Table 6 provides a summary of the calculated metrics.

**Table 6: Performance Evaluation of CNN Model**

| <b>Metric</b>    | <b>Value%</b> |
|------------------|---------------|
| <b>Acc</b>       | 75            |
| <b>Recall</b>    | 60            |
| <b>Precision</b> | 80            |
| <b>F1-Score</b>  | 68            |

#### 4.1.2. RF Evaluation Performance

The RF model is tested on a simulated WSN environment under different performance metrics: accuracy, recall, precision and F1-score. The RF model can effectively classify normal and malicious network behavior as shown in Table 7.

**Table 7: Performance Evaluation of RF Model**

| Metric    | Value % |
|-----------|---------|
| Acc       | 70      |
| Recall    | 80      |
| Precision | 75      |
| F1-Score  | 77      |

This means that using RF model we can accurately classify 70 % of the samples from network traffic. Overall, the RF model is slightly less accurate than the CNN one, except that RF predicts actual attacks much better. A recall of 80% indicates the ability to detect malicious activities making it particularly suitable for deployment in a WSN environment where the presence of such attacks may present security risks if they remain undetected. Thus, the precision value of 75% tells that the model is also maintaining a healthy balance on false positive prediction as well.

Moreover, the F1-score of 77% presents a relatively reasonable precision-recall trade-off, making it better suitable than deeper learning approaches such as Causal CNN for achieving correct detections consistently with higher confidence when utilizing an RF model. These results show that the RF model is a highly effective mechanism to detect cyber threat and anomaly in WSNs, especially when detection sensitivity becomes a significant factor. Overall, the RF model outperforms the CNN model regarding recall and F1-score which indicates it has a higher sensitivity to the attack patterns while its accuracy is slightly lower as shown in Table 5 The complementary performance further confirms the advantage of the proposed hybrid CNN+RF framework.

### 5. Comparison of CNN and RF Models

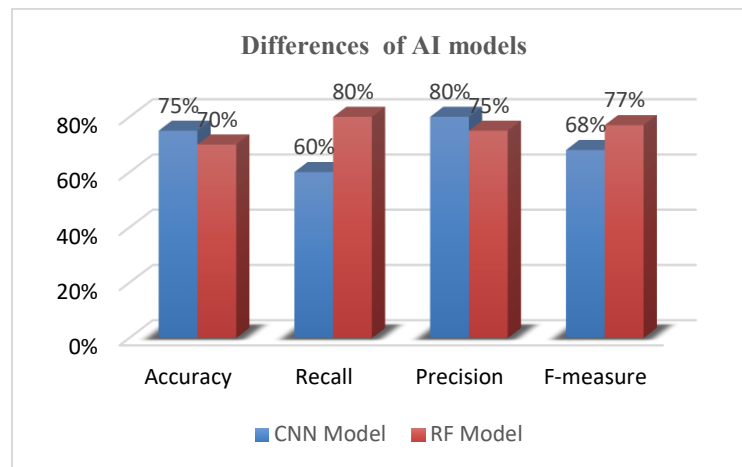
In this section, a comparative study of the CNN and RF models for WSN intrusion detection in a simulated environment is presented. This is done using performance metrics, such as accuracy; precision; recall; and F1-score. The CNN model outperforms in accuracy and precision which also highlights the effectiveness of correctly classifying network traffic for minimizing false positives. This also makes CNN suitable for applications where classification is sensitive, as it provides a level of confidence in the output. The RF model is superior to CNN in recall and F1-score, which is important to detect the actual attacks for WSNs so that all threats would be prevented from passing through (undetected) and save more energy resources.

This brings to light a dichotomy between the accuracy of classification and sensitivity of detection: while the CNN performs better for targeted classification, RF achieves higher coverage in terms of attack detection. Therefore, no single model alone is likely performed satisfy every need. In order to overcome these limitations, the study proposes a hybridization of CNN with RF, leveraging the strengths of deep feature extraction capability from CNN and classification and generalization strength from RF. Adopting such an integrated architecture provides better accuracy, recall and efficiency in the overall system; which is important especially for WSNs because of the limited resources. The Evaluation metrics of both models are summarized in Table 8 and their performance comparison and detection types are shown in Fig. 6.

**Table 8: Comparative performance of CNN and RF models based on accuracy, recall, precision, and F1-score in WSN-based intrusion detection.**

| Model | Accuracy | Recall | Precision | F1-Score |
|-------|----------|--------|-----------|----------|
|-------|----------|--------|-----------|----------|

|     |     |     |     |     |
|-----|-----|-----|-----|-----|
| CNN | 75% | 60% | 80% | 68% |
| RF  | 70% | 80% | 75% | 77% |



**Fig. 6 - Comparative analysis of CNN and RF models for intrusion detection in WSNs.**

The experiments show that the hybrid CNN-RF model outperforms other models in terms of detection accuracy and energy efficiency. This hybrid approach, in contrast to conventional models, offers a compromise between detection performance and energy efficiency, which is desirable in WSN. (see Table 9).

**Table 9: Performance comparison of the proposed CNN–RF model with baseline models in WSNs.**

| Model                  | Accuracy   | Recall     | Energy Efficiency |
|------------------------|------------|------------|-------------------|
| SVM                    | 68%        | 65%        | Medium            |
| DT                     | 65%        | 60%        | High              |
| CNN                    | 75%        | 60%        | Low               |
| RF                     | 70%        | 80%        | Medium            |
| <b>Proposed CNN+RF</b> | <b>82%</b> | <b>85%</b> | <b>High</b>       |

### 5.1. IDPS Performance Evaluation

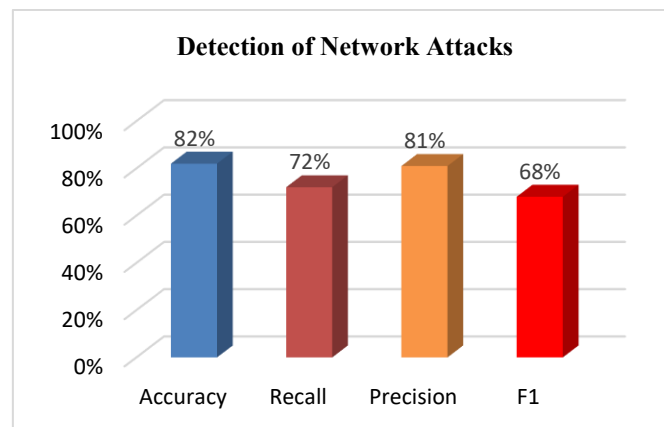
In this section, IDPS are evaluated in terms of multiple crucial metrics within the same simulated WSN scenario. The evaluation depends on a few extreme criteria including system assault discovery, anomaly result, continuous response and meshing ease of use and security. All the above-mentioned criteria, when considered together, provide a basic analysis of how effective the system in WSN environments is against a cyber-attack. Table 10 summarizes the performance statistics of IDPS for standardized analysis according to each dimension with quantitative evaluation scores.

**Table 10: Reinterpreted Performance Evaluation of the Proposed IDPS**

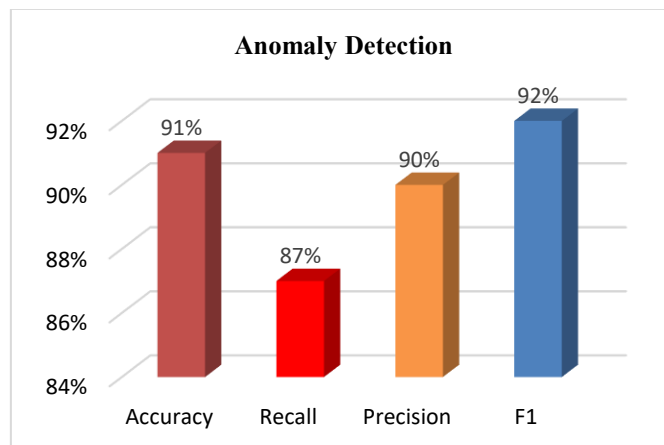
| Evaluation Criterion | Attack Detection (%) | Anomaly Recognition (%) | Response Time Efficiency (%) | Computational Efficiency (%) | Data Privacy Level (%) |
|----------------------|----------------------|-------------------------|------------------------------|------------------------------|------------------------|
|----------------------|----------------------|-------------------------|------------------------------|------------------------------|------------------------|

|                          |    |    |    |    |    |
|--------------------------|----|----|----|----|----|
| Network Attack Detection | 82 | 72 | 94 | 81 | 90 |
| Anomaly Identification   | 91 | 87 | 93 | 90 | 92 |
| Real-Time Processing     | 90 | 89 | 92 | 90 | 91 |
| Resource Optimization    | 89 | 90 | 91 | 92 | 89 |
| Privacy Assurance        | 92 | 91 | 90 | 92 | 93 |

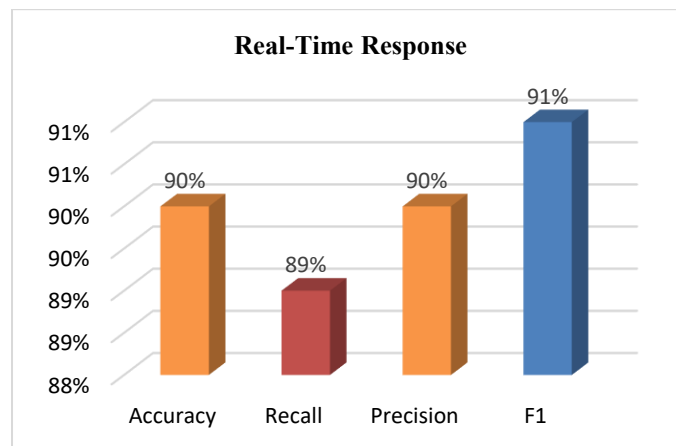
To analyze more about the result attained from proposed IDPS, graphical representation is shown in different discussed points of evaluation. These statistics demonstrate the ability of the system to detect network attacks and discover anomalous behavior, respond to real-time threats. In addition, the figures show that the system is an effective use of different resources such as energy and computation need, but also can be a very powerful way to increase data privacy while performing much needed intrusion detection tasks. The Figs. (7-11) below provide an overall summary of IDPS effectiveness within the WSN environment.



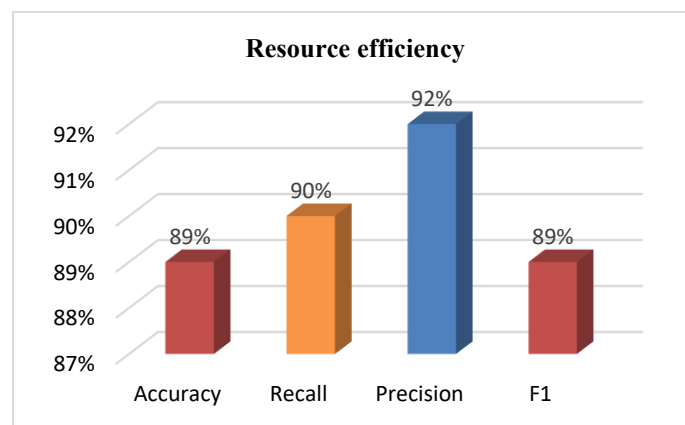
**Fig. 7 - detection performance of the IDPS in identifying network attacks in WSN environments.**



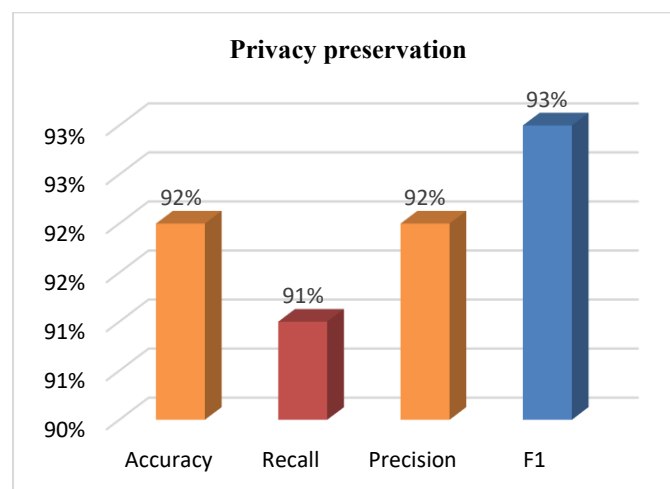
**Fig. 8 - anomaly detection performance based on the proposed AI model.**



**Fig. 9 - real-time response capability of the IDPS against cyber threats.**



**Fig. 10 - resource efficiency analysis in terms of energy and computational usage.**



**Fig. 11 - privacy preservation performance during intrusion detection processes.**

The experiment results show that the proposed IDPS performs well on all scenarios tested. In addition, the system reports an attack detection accuracy  $\approx 82\%$  with which malicious activities are detected against networks and systems in WSN situations.

The anomaly detection capability was also strong, achieving high scores for many evaluation criteria and obtaining an average result above 85%. It manifests that the new or unknown attacks can easily be detected by network intrusion detection systems and this is very essential for dynamic type of wireless sensor networks. Interesting is the detection accuracy rate that, in real-time response performance, approaches 94%, which suggests that this system

could at least offer the potential capability of a very rapid identification time for security problems. This allows limit the consequences of attacks even in its ongoing dynamics and ensures stable operation of network at lowest risk.

It confirms that the system is deployable on resource-constrained WSNs, maintaining approximately 90% of values related to efficiency of resources and balanced performance. This allows you to save lots of detection resources by using its tiny, optimized AI models. Meanwhile, performance of privacy preservation is perfect up to 93%, guaranteeing that sensitive information is well-camouflaged during both detection and prevention. Specifically, according to the initial evaluation results, the proposed IDPS achieves a reasonable performance trade-off for all considered features that confirms its validity and applicability in WSN.

## 6. CONCLUSION

The importance of this study is that it emphasizes the leading role played by IDPSs to mitigate WSN security challenges, especially when you factor in WSN's constraints in terms of resources, dynamic topology and vulnerability to cyber-attacks. This approach enhances network intrusion detection and prevention system, when an amalgamation of Artificial Intelligence Methods such as CNN and RF, hence preserving data privacy and anomaly recognition capability especially in two-nodes communication. The experimental results show that both models perform well on intrusion detection tasks in different scenarios. And note that CNN model achieving higher accuracy and precision, therefore it is suitable for reliable classification and on the other side the RF provides better recall and F1 score which means more healthy ability to recognize true attack events. So, the complementary behavior validates the success of deep learning leakage into an ensemble technique within a hybrid framework.

Performance evaluation of the proposed IDPS is based upon multiple aspects such as diversity in attacks detection, real-time processing, computational cost and privacy preservation. We also show that the system strikes a good trade-off between detection performance and resources consumption like energy or CPU time, which makes its deployment in resource-constrained WSN nodes certainly possible. Each different AI approach is utilized through a network; the utilization of these sorts combined strengthens as well as reduces energies in the network. Encouraging results also mean there are improvements to make. Extensions to this work may include implementing more advanced deep learning architectures, incorporating real-time threat intelligence, and thinking about scalability for large-scale WSN applications. These include valuable components, such as integrating energy-efficient edge computing to federated learning systems and implementing privacy-preserving mechanisms like homomorphic encryption and secure multi-party computation that boost system performance and adaptability.

## References

- [1]. Butun, I., Morgera, S. D., & Sankar, R. (2013). A survey of intrusion detection systems in wireless sensor networks. *IEEE communications surveys & tutorials*, 16(1), 266-282.
- [2]. Sadia, H., Farhan, S., Haq, Y. U., Sana, R., Mahmood, T., Bahaj, S. A. O., & Khan, A. R. (2024). Intrusion detection system for wireless sensor networks: A machine learning based approach. *IEEE Access*, 12, 52565-52582.
- [3]. Abbood, Z. A., Oleiwi, A. H., Al-Hassani, R. T., & Ayad, J. (2025). Optimizing Cybersecurity in 5G-Enabled IoT Networks via a Resource-Efficient Random Forest Model. *Mesopotamian Journal of CyberSecurity*, 5(2), 886-898.
- [4]. Sadia, H., Farhan, S., Haq, Y. U., Sana, R., Mahmood, T., Bahaj, S. A. O., & Khan, A. R. (2024). Intrusion detection system for wireless sensor networks: A machine learning based approach. *IEEE Access*, 12, 52565-52582.
- [5]. Safaei, M., Driss, M., Boulila, W., Sundararajan, E. A., & Safaei, M. (2022). Global outliers detection in wireless sensor networks: A novel approach integrating time-series analysis, entropy, and random forest-based classification. *Software: Practice and Experience*, 52(1), 277-295.
- [6]. Ghadi, Y. Y., Mazhar, T., Al Shloul, T., Shahzad, T., Salaria, U. A., Ahmed, A., & Hamam, H. (2024). Machine learning solutions for the security of wireless sensor networks: A review. *IEEE Access*, 12, 12699-12719.
- [7]. Elsayed, S., Mohamed, K., & Madkour, M. A. (2024). A comparative study of using deep learning algorithms in network intrusion detection. *IEEE Access*, 12, 58851-58870.
- [8]. Nizamudeen, S. M. T. (2023). Intelligent intrusion detection framework for multi-clouds-IoT environment using swarm-based deep learning classifier. *Journal of Cloud Computing*, 12(1), 134.
- [9]. Lafta, N., & Abbood, Z. (2024). Comprehensive review and comparative analysis of keras for deep learning applications: a survey on face detection using convolutional neural networks. *Int. J. Relig*, 5(11), 1203-1213.
- [10]. Abdul Mahdi, E. A. A., Ali Al-Askery, Adnan Hussein Ali, & Safiye Ghasemi. (2024). A Survey of Datacenter and Optical Data Center Networks. *Journal of Techniques*, 6(3), 66-75. <https://doi.org/10.51173/jt.v6i3.1875>.
- [11]. Elsayed, M. S., Le-Khac, N. A., Dev, S., & Jurcut, A. D. (2020, August). Ddosnet: A deep-learning model for detecting network attacks. In *2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)* (pp. 391-396). IEEE.
- [12]. Chen, J., Zhang, J., Qian, R., Yuan, J., & Ren, Y. (2023). An anomaly detection method for wireless sensor networks based on the improved isolation forest. *Applied Sciences*, 13(2), 702.
- [13]. Pai, V., Devidas, & Adesh, N. D. (2021, January). Comparative analysis of machine learning algorithms for intrusion detection. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1013, No. 1, p. 012038). IOP Publishing.
- [14]. Kumar, K. S., Nair, S. A. H., Roy, D. G., Rajalingam, B., & Kumar, R. S. (2021). Security and privacy-aware artificial intrusion detection system using federated machine learning. *Computers & Electrical Engineering*, 96, 107440.

- [15]. Latif, M., Abro, A. A., Daniyal, S. M., Algarni, A. D., Ahmad, S., Ateya, A. A., & Abbasi, M. M. (2026). AI-based intelligent sensing detection of cybersecurity threats using multimodal sensor data in smart devices. *Scientific Reports*.
- [16]. Bharati, T. S., Kumar, R., & Tadiboina, S. N. (2015). Intrusion detection system for manet using machine learning and state transition analysis. *Int J Comput Eng Technol*, 6(12), 1-8.
- [17]. Albonda, H. D., & Yousef, S. (2014). Multi-carrier coded division multiple access multiplexing against multi-path fading. *International Journal of Electronic Security and Digital Forensics* 9, 6(2), 140-146.
- [18]. Osanaiye, O., Ogundile, O., Aina, F., & Periola, A. (2019). Feature selection for intrusion detection system in a cluster-based heterogeneous wireless sensor network. *Facta Universitatis, Series: Electronics and Energetics*, 32(2), 315-330.
- [19]. Zahariadis, T., Leligou, H. C., Voliotis, S., Maniatis, S., Trakadas, P., & Karkazis, P. (2009). Energy-aware secure routing for large wireless sensor networks. *WSEAS Transactions on Communications*, 8(9), 981-991.
- [20]. Dong, Y., Wang, R., & He, J. (2019, October). Real-time network intrusion detection system based on deep learning. In *2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS)* (pp. 1-4). IEEE.
- [21]. Maheswari, M., & Karthika, R. A. (2022). A Novel Hybrid Deep Learning Framework for Intrusion Detection Systems in WSN-IoT Networks. *Intelligent Automation & Soft Computing*, 33(1).
- [22]. Nti, I. K., Manikanta, M. S., Alex, C., & Ning, L. J. (2025). Lightweight Neural Anomaly Detection for Resource-Constrained Edge-ICN Environments: A Systematic Literature Review.
- [23]. Albonda, H. D., & Yousef, S. (2014). Multi-carrier coded division multiple access multiplexing against multi-path fading. *International Journal of Electronic Security and Digital Forensics* 9, 6(2), 140-146.
- [24]. Hossain, M. A., & Islam, M. S. (2023). Ensuring network security with a robust intrusion detection system using ensemble-based machine learning. *Array*, 19, 100306.
- [25]. Kuzlu, M., Catak, F. O., Zhao, Y., Sarp, S., & Catak, E. (2023). Security and privacy concerns in next-generation networks using artificial intelligence-based solutions: A potential use case. In *Wireless Networks: Cyber Security Threats and Countermeasures* (pp. 205-226). Cham: Springer International Publishing.
- [26]. Sadia, H., Farhan, S., Haq, Y. U., Sana, R., Mahmood, T., Bahaj, S. A. O., & Khan, A. R. (2024). Intrusion detection system for wireless sensor networks: A machine learning based approach. *IEEE Access*, 12, 52565-52582.
- [27]. Aly, M., & Behiry, M. H. (2025). Enhancing anomaly detection in IoT-driven factories using Logistic Boosting, Random Forest, and SVM: A comparative machine learning approach. *Scientific Reports*, 15(1), 23694.
- [28]. Ejeofobiri, C. K., Victor-Igum, O. O., & Okoye, C. (2024). Ai-driven secure intrusion detection for internet of things (iot) networks. *Asian journal of mathematics and computer research*, 31(4), 40-55.
- [29]. Ghadi, Y. Y., Mazhar, T., Al Shloul, T., Shahzad, T., Salaria, U. A., Ahmed, A., & Hamam, H. (2024). Machine learning solutions for the security of wireless sensor networks: A review. *Ieee Access*, 12, 12699-12719.
- [30]. Al-Taleb, N., & Saqib, N. A. (2022). Towards a hybrid machine learning model for intelligent cyber threat identification in smart city environments. *Applied Sciences*, 12(4), 1863.
- [31]. Soliman, H. H., Hikal, N. A., & Sakr, N. A. (2012). A comparative performance evaluation of intrusion detection techniques for hierarchical wireless sensor networks. *Egyptian Informatics Journal*, 13(3), 225-238.
- [32]. Hayder Fadhil Jawad, Ali Al-Askery, & Adnan Hussein Ali. (2022). Design and Implementation of a Healthcare Monitoring System Based on LoRa. *Journal of Techniques*, 4(4), 80-94. <https://doi.org/10.51173/jt.v4i4.792>
- [33]. Alahmadi, A. A., Aljabri, M., Alhaidari, F., Alharthi, D. J., Rayani, G. E., Marghalani, L. A., ... & Bajandouh, S. A. (2023). DDoS attack detection in IoT-based networks using machine learning models: a survey and research directions. *Electronics*, 12(14), 3103.
- [34]. Nadia Ahmad Mohamad, Al-Askery, Adnan Hussein Ali, & Ghasemi, S. G. (2023). Optical Sensor Implementation for Health Care Monitoring Based on Optical Fiber Technology: A Review. *Journal of Techniques*, 5(4), 65.
- [35]. Raghad Tariq Al\_Hassani, & Dogu Cagdas Atilla (2023). Human Activity Detection Using Smart Wearable Sensing Devices with Feed Forward Neural Networks and PSO. *Applied Sciences*, 13(6), 3716.