Journal of Intelligent Systems and Internet of Things
Vol. 17, No. 01, PP. 219-238, 2025
DOI: https://doi.org/10.54216/JISIoT.170116

# Explainable Artificial Intelligence Driven Intrusion Detection System for Enhancing Reliability and Interpretability in IoT Based Network Security Solutions

**Purshottam J. Assudani[1,*], N. V. S. Pavan Kumar[2], K. Mohanambal[3], R. Chitra[3]**

[1]Assistant Professor, School of Computer Science and Engineering, Ramdeobaba University, Nagpur, Maharashtra, India

[2]Associate Professor, Dept. of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India

[3]Asst. Professor, Dept. of CSE, Velammal Engineering College, Chennai, TN, India

Emails: assudanipj@rknec.edu; nvspavankumar@kluniversity.in; mohanambal@velammal.edu.in; chitrar05@gmail.com

**Abstract**

The implementation of Intrusion Detection Systems (IDS) remains crucial for network security yet high-dimensional data alongside class imbalance issues decrease their functionality. Machine learning-based IDS models, which use traditional approaches experience difficulties in providing explanations about their prediction results. An IDS framework enhancement with explainable AI (XAI) methods aims at improving the system's transparency throughout this study. The data processing includes KNN imputation combined with K-Means SMOTE to handle missing information and class imbalance problems. When selecting features the model uses a merged methodology combining Pearson Correlation with Mutual Information and Sequential Forward Floating Selection (SFFS) algorithms for optimization. Light Gradient Boosting Model (LGBM) serves as the classification model that produces higher accuracy than competing methods with 90.71% for UNSW-NB 15 and 96.98% for CICIDS-2017. By using SHAP-based explain ability, the system provides worldwide and specific model interpretations that enable users to trust IDS prediction results. The experimental findings validate that the proposed methodology succeeds in simplifying the system while improving its classification functionality and delivering stronger interpretability properties to tackle weaknesses of current IDS technologies. The examination presents important findings for the development of secure network protection technologies, which operate with transparency.

**Received: January 31, 2025 Revised: March 01, 2025 Accepted: April 20, 2025**

**Keywords:** Intrusion Detection System (IDS); Explainable AI (XAI); Machine Learning (ML); Feature Selection; Class Imbalance; Light Gradient Boosting Model (LGBM)

## 1. Introduction

Digital expansion of networked devices in smart homes and transportation and manufacturing and healthcare domains drove an unprecedented surge of data transmission in modern times. Network architecture development alongside technological progress creates an urgent need to protect all confidential and sensitive information transferred across those networks [1]. The combination of multiplying network data volumes together with strong advanced cyber threats has rendered standard security tools including passwords and computer filters insufficient in protecting against modern cyber-attacks.

Systems-based Intrusion Detection (IDS) emerged as crucial security elements, which protect network infrastructure against continuous growing cybersecurity threats. IDS began their existence when Anderson Jim first introduced them in 1980 and have developed into advanced security systems that inspect and process network

data to detect threats [2]. The IDS development split into deployment-based and detection-based models throughout the years while providing exact strength points and specific constraints. Conventional IDS systems have progressed through time but still encounter difficulties in processing current threats, extensive network traffic, and multivariate security data, which requires advanced and transparent security solutions [3]. The IDS belongs to the Deployment category and operates under the Detection system. The illustration of IDS classification appears in Figure 1.

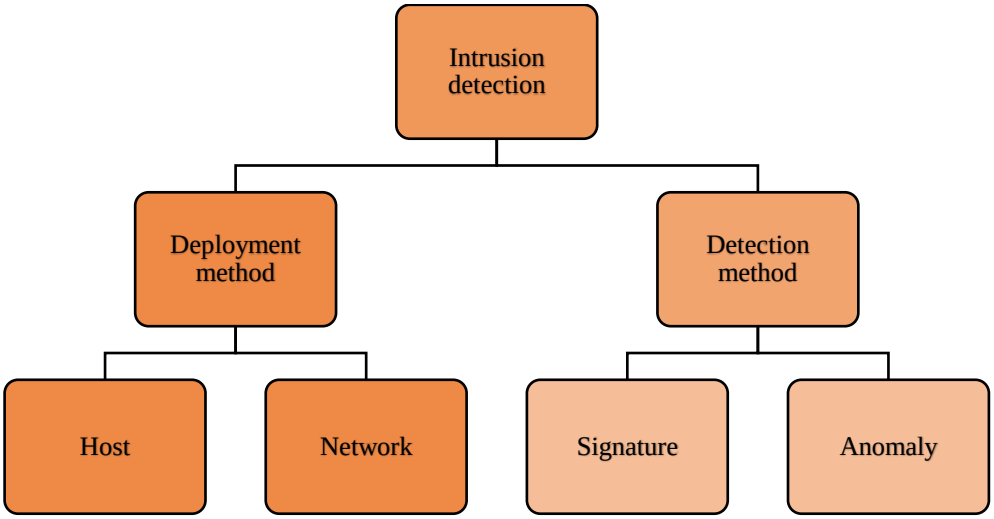


**Figure 1.** Illustration of IDS classification

### 1.1 Growing Threat Landscape

Rising digital communication dependence has made cyberattacks more dangerous because cyber adversary organizations use complex methods to exploit weak network points [4]. Various attack vectors allow malicious actors to accomplish network security breaches by using phishing techniques along with ransomware spread and malware distribution and Distributed Denial-of-Service (DDoS) assaults [5]. Speeding up the digital age has directed the majority of ransomware attacks toward essential sectors such as finance and government operations together with transportation infrastructure, which proves the necessity to boost security protocols. The growing number of cyber threats requires immediate action in building resilient intrusion detection systems because these threats now appear more frequently.

Traditional security measures such as firewalls do not fully protect networks from emerging and new threats, which is why authentication protocols and encryption techniques prove insufficient to detect these threats [6]. Since cybercriminals keep refining their attack, approaches security solutions need to maintain an equivalent advancement pace. Inherit benefit IDS have become necessary tools to detect analyse and minimize cyber threats by utilizing network action analysis and detecting irregular conduct.

### 1.2 Intrusion Detection System (IDS) Classification

IDS operates within two main classification groups, which include deployment-based and detection-based systems. Deployment-based IDS consists of two individual types including host-based and network-based systems. The Host-based Intrusion Detection Systems (HIDS) function by inspecting device-specific incidents to examine system logs and application operations and system settings to detect unauthorized or malicious activities [7]. Security breaches trigger alert notifications through these systems that have predefined behaviour reference points.

Network-based Intrusion Detection Systems (NIDS) function at the network level where they scan data packets moving through the network to identify suspicious patterns and attack signatures as well as anomalies [8]. The security standpoint of NIDS extends beyond HIDS by conducting analysis across entire network traffic to discover potential threats.

The detection-based IDS includes two main approaches, which are signature-based and anomaly-based detection. Signature-basedIDS distinguishes between legitimate and malicious traffic through attack signatures, which are predefined within its system. The detection systems maintain a high standard of identifying existing threats yet encounter problems when they encounter unknown or zero-day attacks because they need regular database updates [9]. Anomaly-based IDS creates behavioural patterns from normal traffic that enables it to detect abnormal

deviations from defined baselines. Anomaly-based IDS demonstrate strong capability in detecting unknown threats although they produce substantial numbers of incorrect alarms that reduce their operational effectiveness.

### 1.3 Challenges in Intrusion Detection

The utilization of IDS for network security presents multiple hurdles that reduce their effectiveness for robust prevention. The main challenge arises because cyber threats continuously evolve which forces IDS systems to automatically detect new types of attacks [10]. Traditional IDS systems fail to catch up with modern evasion techniques deployed by attackers, which produces opportunities for threats to breach security systems. System operators must overcome the problem of handling overwhelming network traffic flow. The tremendous expansion of internet users coupled with digital transactions produces excessive network data that proves challenging to IDS [11]. These systems of high internet traffic require advanced computation models to avoid system breakdowns and accomplish fast threat recognition.

IDS systems face the challenge of working with extensive data containing many features that affect network behavioural analysis. Finding optimal features for intrusion detection is challenging because unimportant characteristics add either performance issues or lower IDS performance accuracy. The selection and extraction of features from data plays an essential role in IDS model optimization because it creates better detection outcomes with reduced resource consumption [12-13]. The problem of class imbalance in network traffic data proves to be a major obstacle during analysis. The ratio of benign traffic over malicious traffic creates obstacles for IDS to learn suitable intrusion patterns because benign instances outnumber malicious ones in most cases. Traditional machine learning algorithms face difficulties working with unbalanced datasets because the resulting classifications become distorted and due to which detection ability deteriorates.

### 1.4 Role of Explainable AI in Intrusion Detection

The rise of Explainable Artificial Intelligence (XAI) represents a transformational solution against the problems that face intrusion detection systems. The application of XAI techniques makes IDS models more easily understandable for security analysts to build trust in system reaction patterns. IDS systems with explainability capabilities produce comprehensible threat explanations, which enhance human-operated threat management and defines strategies [14].

The network traffic analysis of XAI-driven IDS relies on advanced machine learning together with deep learning models, which maintain interpretability capabilities. Feature selection and ranking tools act as important performance boosters for IDS systems by selecting the threat detection relevant attributes [15]. A combination of multiple feature selection methods using mutual information and permutation importance and Shapley Additive Explanations (SHAP) allows IDS to develop the best possible feature models that boost its classification precision.

These black-box models require XAI techniques for making their decision-making processes comprehensible since they remain complex and non-interpretable [16]. The application of Local Interpretable Model-agnostic Explanations (LIME) and SHAP analysis enables IDS to reveal precise information about feature significance as well as why anomalies are identified through clear explanation methods.

This research follows an organizational structure that includes the following section breakdown: The paper begins with a literature review in Section 2 to explore related works while highlighting the knowledge gaps. In Section 3 of the research, the objectives become specified through clear definitions that describe the study's intended outcomes. The section explores the research motivations by illustrating why the problem is essential in modern circumstances. In this section, the research describes the classifier models, which served as the study foundation including their techniques and implementation methods. Section 6 presents model performance evaluations with experimental results containing performance metrics along with analytical assessments. Section 7 serves as the concluding segment, which summarizes the research while providing future research directions and major work contributions.

## 2. Related Work

Modern networks require IDS as an essential component because cyber threats have evolved in their complexity. The evolution of cybersecurity threats contains malware and denial-of-service (DoS) attacks and ransomware and insider threats exceeds the capabilities of conventional security rules. Network traffic monitoring via IDS detects possible threats with the help of Machine Learning (ML), Deep Learning (DL) and Explainable Artificial Intelligence (XAI) techniques [17].

The application of ML models for network anomaly detection becomes automated when they learn patterns from attack data records and DL models extract complex patterns from large dataset analysis. The lack of transparency in these models prompted experts to create XAI techniques that provide security analysts with interpretability features.

The research study examines IDS in detail by investigating three key areas, which include traffic data collection and class imbalance and feature selection together with ML/DL-based IDS systems and hybrid models and XAI techniques [18]. The paper aims to evaluate recent breakthroughs and obstacles in IDS solution development. The survey finds ways hybrid system implementations composed of different techniques perform to boost detection capabilities and decrease misleading outcomes. This part highlights the necessity of real-time attack mitigation, which must be supplemented by enhanced scalability and ability to confront new security threats.

The IDS research investigates multiple domains starting with dataset selection then proceeding to feature engineering and moving onto ML/DL methods and ending with XAI approaches [19]. The following table demonstrates how IDS research has consolidated all major research domains into one viewpoint.

The research achievements of IDS development face multiple unresolved problems:

- The real-time analysis of network traffic proves challenging for most IDS products since they exhibit delayed responses to ongoing attacks.
- The growing network data volumes require security solutions with scalable features, which maintain performance quality even at large deployment scales.
- Evasion attacks persist as attackers develop new ways to evade IDS detection thus making it necessary for IDS models to adapt capabilities that prevent emerging attack strategies.
- There is a trade-off between XAI model interpretation capabilities and their performance levels or operational complexity.
- Feasibility challenges emerge when trying to integrate IDS frameworks with existing security systems because framework designers must create flexible modular designs.

**Table 1:** Comprehensive Literature Survey

| Research Area | Key Focus | Techniques Used | Benefits | Challenges |
|---|---|---|---|---|
| Traffic Data Collection [20] | Use of benchmark datasets for IDS evaluation | NSL-KDD, UNSW-NB15, CIC-IDS2017, ToN IoT, CIC IoT 2023 | Provides diverse real-world attack scenarios | Data redundancy, outdated attack patterns, limited real-time applicability |
| Class Imbalance Handling | Techniques to balance attack and normal traffic data | SMOTE, Borderline-SMOTE, GANs, ADASYN, Random Oversampling | Reduces bias towards majority classes, improves detection [21] | May introduce synthetic noise, increases computational overhead, reduces generalizability |
| Feature Selection | Identifying relevant features to enhance detection accuracy | Filter (Correlation, Mutual Information), Wrapper (Genetic Algorithms, Recursive Feature Elimination), Embedded (Tree-based models) [22] | Reduces dimensionality, improves computation time, removes irrelevant features | Risk of losing important features, complex parameter tuning, domain dependency |
| Machine Learning-Based IDS | ML models for intrusion detection [23] | SVM, Decision Trees, KNN, Random Forest, LightGBM | High accuracy, interpretable models, effective for structured data | Overfitting, requires manual feature engineering, struggles with high-dimensional data |

| | | | | |
|---|---|---|---|---|
| Deep Learning-Based IDS | DL models for improving IDS accuracy | CNN, Autoencoders, LSTM, GANs | Automated feature extraction, high detection rate, effective for complex patterns [24] | High computational cost, requires large datasets, lack of interpretability |
| Hybrid Deep Learning Models | Combining multiple DL models for better detection [25] | CNN+LSTM, AE+LSTM, Sparse AE+DNN | Captures spatial and temporal patterns, robust against evolving attacks, improves generalization | Increased training time, complex hyperparameter tuning, risk of model instability |
| Explainable AI in IDS | Enhancing model transparency and interpretability | SHAP, LIME, Decision Trees, Feature Importance Analysis [26-28] | Improves trust in IDS decisions, identifies key influencing features, aids security analysts | Limited real-time deployment, difficulty in explaining complex DL models, potential performance trade-offs |

The study of IDS shows increasing use of ML alongside DL technologies with XAI techniques. The performance of IDS receives enhancement from implementation of feature selection and class balancing and hybrid modelling approaches but existing research questions as shown in table 1 focus on scalability issues and real-time detection alongside explainability [29-31]. Researchers need to create IDS models that combine efficiency and scalability and interpretability while staying resistant to updated cyber dangers.

## 3. Objectives of Research

The research aim establishes the development of an Intrusion Detection System improvement to achieve better detection accuracy and false positive reduction through Explainable AI (XAI) developments. The research targets Intrusion Detection System challenges through its objectives that focus on high-dimensional data problems along with imbalanced class distributions and the lack of interpretability within machine learning detection models.

The research establishes the following set of objectives to reach its main goal.

- Network data preprocessing requires the implementation of methods to clean data while normalizing values and handling missing entries in order to establish model reliability.
- The detection performance for various attack groups becomes improved when K-Means SMOTE techniques are applied to balance datasets for addressing class imbalance.
- A hybrid feature selection approach must be developed using Pearson Correlation coupling with Mutual Information together with Sequential Forward Floating Selection (SFFS) to choose valuable features and decrease computational demands.
- A Light Gradient Boosting Machine (LGBM) is installed and evaluated for its ability to deliver precise attack detection.
- A local and global explanation system based on SHAP should be integrated into the IDS framework for transparent monitoring of decision-making procedures.

The research findings work toward enhancing IDS performance with stronger reliability, which leads to more transparent and effective network protection systems.

## 4. Motivation of the Research

Modern digital network growth resulted in advanced cybersecurity threats that deliver substantial risks to both organizations and individual users. Intrusion Detection Systems struggle to identify new attacks because they need to handle high-dimensional data, manage class imbalance in data sets and their machine learning models lack interpretability during operation [32]. Security applications with black-box models receive limited trust because these effective systems lack decision transparency.

The research goal aims to improve IDS functionality and explainability through Explainable AI (XAI) system integration. Efforts focus on solving three critical problems related to false positives together with performance

complexity and feature redundancy to establish an IDS system with enhanced clarity and operational efficiency and trustworthiness.

The present IDS solutions do not achieve appropriate dataset balance together with optimized feature selection that ensures generalization between diverse network conditions [33]. This research develops IDS through SMOTE data balancing with K-Means clustering as well as hybrid feature selection along with SHAP-based explain ability, which detects attacks precisely while demonstrating logical reasoning for each prediction. The findings enable cybersecurity experts to take better course of action, which results in enhanced protection of network systems and improved security threat prevention.

## 5. Proposed Work

The proposed IDS framework develops an effective intrusion detection capability through machine learning integration with XAI to achieve improved explainability and efficiency alongside accuracy. The framework handles important problems such as disparate classes and high dimensional space together with interpretability limitations through advanced preprocessing methods and combination feature selection along with an LGBM-based resistant classifier. This paper describes the development methodology for IDS where equations along with algorithms depict the implementation process and particular emphasis is given to real-time detection enhancement and computational performance optimization.

### 5.1 Data Preprocessing

Intrusion Detection Systems (IDS) depend on data preprocessing as an essential first step in their machine learning pipeline to address the common problems of network traffic data which includes missing values and noise together with redundant information alongside class imbalance issues. The performance of the model is affected negatively through issues that introduce bias while also increasing complexity and reducing generalization ability. Data preprocessing serves to refine the dataset through several procedures that cleans and transforms data into a format suitable for the classification model to identify meaningful patterns effectively.

The procedural sequence for data preprocessing includes:

- Handling Missing Values
- Feature Normalization
- Class Imbalance Handling

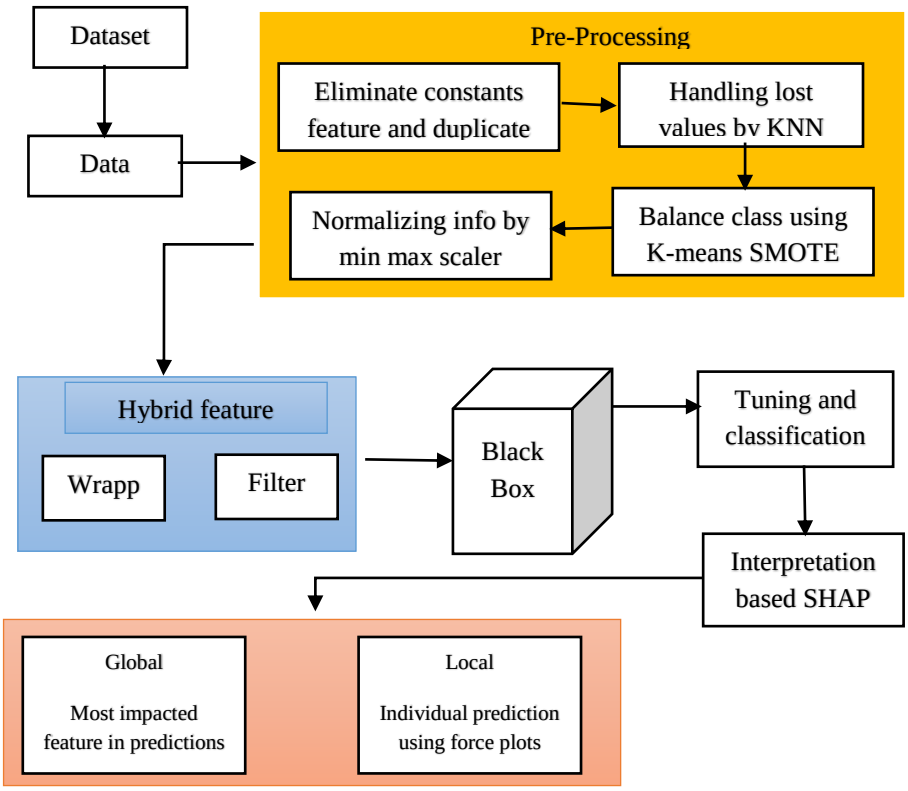


**Figure 2.** Illustration framework of proposed Intrusion detection system

### 5.1.1 Handling Missing Values Using KNN Imputation

Network datasets experience data loss because of three primary reasons including packet loss and incomplete logging alongside hardware malfunctions. Accurate handling of missing values stands essential to ensure data consistency and reinforce the reliability of the models. Using mean or median substitutions as a basic strategy to handle missing data results in inappropriate modification of data distribution. K-Nearest Neighbours (KNN) Imputation acts as our method for data imputation because it calculates values through neighbouring observations.

The distance between data points $X_i$ and $X_j$ is measured through Euclidean distance.

$$D(X_i, X_j) = \sqrt{\sum_{k=1}^{n} w_k \left(x_{ik} - x_{jk}\right)^2} \quad (1)$$

The estimation of missing value $x_{ik}$ depends on calculating the weighted average from its K nearest neighbour's.

$$\hat{x}_{ik} = \frac{\sum_{j=1}^{K} w_j x_{jk}}{\sum_{j=1}^{K} w_j} \quad (2)$$

Here D ($X_i$, $X_j$) = Euclidean distance, $w_k$ = weight factor, n = no of features, k = no of neighbors.

A basic KNN Imputation operation has a computational complexity of $O(n^2)$ because it calculates all pair-wise distances across all missing values. The application of KD-Trees or Ball Trees results in an optimized O (n log n) complexity for the KNN Imputation algorithms.

Algorithm 1: KNN Imputation for Missing Values

> Input: Dataset with missing values, K (number of neighbors)
>
> Output: Dataset with imputed values
>
> Find the K closest neighbors from the dataset by calculating Euclidean distance at every missing value point.
> Computing the weighted mean requires use of non-missing values found in neighboring observations.
> The computed weighted mean serves to fill in each missing value.
> The procedure continues until all absent values receive proper replacement.
> Return the preprocessed dataset.

### 5.1.2 Feature Normalization Using Min-Max Scaling

Network datasets contain features with different numeric ranges including packet size in contrast to connection duration. The learning process may become biased because features with larger magnitudes will gain superiority if normalization is not performed. Min-Max Scaling transforms values into the [0,1] scale to create an environment that provides equal weighting of all the features.

$$X' = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \quad (3)$$

Normalization takes a computational complexity of O(n) to complete a single scan through all dataset entries for min/max value determination.

### 5.1.3 Handling Class Imbalance Using K-Means SMOTE

Attack sample frequencies are much lower than normal traffic patterns within network intrusion detection systems which results in biased modelling. The K-Means Synthetic Minority Over-Sampling Technique (SMOTE) solves this problem through synthetic sample creation in minority class sparse areas which boosts model reliability.

Step 1: Clustering: The dataset receives K-Means clustering to divide it into K clusters.

$$\mu_k = \frac{1}{N_k} \sum_{i \in C_k} X_i \quad (4)$$

Step 2: Imbalance Ratio Computation: The SMOTE-based oversampling process focuses on clusters that present low Imbalance Ratio.

$$IR(f) = \frac{|minority(f)|}{|majority(f)|} \quad (5)$$

Step 3: SMOTE-Based Oversampling: The process produces synthetic sample X′ for each minority sample Xi through the following procedure:

$$X' = X_i + \lambda(X_j - X_i), \quad \lambda \sim U(0,1) \qquad (6)$$

Here $\mu_k$ = centroid of cluster**,** $N_k$ = no of points in cluster, $X_i$ and $X_j$= minority-class points.

Algorithm 2: K-Means SMOTE

| |
|---|
| Input: Imbalanced dataset, K (number of clusters)<br>Output: Balanced dataset<br>Cluster the dataset into K groups.<br>Determine the imbalance ratio of every cluster group.<br>Identify minority clusters requiring oversampling.<br>The clusters receive synthetic samples through SMOTE mechanism.<br>Return the balanced dataset. |

### 5.2 Hybrid Feature Selection

The process of feature selection enhances efficiency by removing redundant features because it minimizes computational requirements while stopping overfitting. The proposed hybrid method integrates:

- Using Pearson Correlation Coefficient (PCC) to detect linear correlations between different features is part of this selection process.
- The retention of most informative features is achieved through Mutual Information (MI).
- Sequential Forward Floating Selection (SFFS) for dynamic feature subset selection.

#### 5.2.1 Pearson Correlation Coefficient (PCC)

The Pearson Correlation Coefficient (PCC) serves as a quantitative indicator for measuring the linear connection between two numerical elements. Machine learning algorithms use PCC to find multicollinearity between features thus preventing performance-degrading redundant attributes from entering models.

PCC is expressed as:

$$\rho(X,Y) = \frac{Cov(X,Y)}{\sigma_X \sigma_Y} \qquad (7)$$

The model achieves better efficiency by eliminating features with absolute correlation values exceeding $|\rho|>0.9$ during feature selection.

Here $Cov(X,Y)$ = covariance of features, $\sigma_X$ and $\sigma_Y$ = standard deviations.

#### 5.2.2 Mutual Information (MI)

MI functions as a non-linear method to evaluate dependency between two random variables. The measurement of information sharing between two features by Mutual Information provides detection capabilities beyond Pearson Correlation Coefficient.

The MI measurement between variables A and B follows the following equation:

$$I(A,B) = H(A) + H(B) - H(A,B) \qquad (8)$$

Here $H(A)$, $H(B)$ = entropy values, $H(A,B)$ = joint entropy.

A higher Mutual Information measurement signals that the features display increased interdependency. MI surpasses PCC because it uncovers linear as well as non-linear feature dependencies which results in superior feature selection performance for complex data.

Features with minimal MI values have minimal predictive potential thus the model drops them to increase system performance and prediction effectiveness.

#### 5.2.3 Sequential Forward Floating Selection (SFFS)

Sequential Forward Floating Selection (SFFS operates as a wrapper-based method for feature selection which chooses optimal features dynamically to enhance model performance. To address redundancy when used with Sequential Forward Selection (SFS) the method extends the framework by enabling features to become removable at any stage.

The algorithm works iteratively:

Inclusion step: Among all possible features the selection step focuses on adding the one which generates the best model performance level.

Conditional exclusion step: Previous features will be removed from the subset when they fail to make significant contributions to model performance.

The formulation for feature subset selection presents itself as:

$$F = \underset{g \in D4}{\operatorname{argmax}} \omega(Z_r \cup g) \quad (9)$$

Here $w(Z_r)$ = model evaluation, g = candidate feature, D = full feature set.

SFFS both prevents problems of overfitting and optimizes model performance by maintaining automatic dynamic selection of features.

Algorithm 3: Hybrid Feature Selection

Input: Dataset with features

Output: Optimal feature subset

The removal of features with high inter-correlations occurs through PCC analysis.
The computation of MI allows for identifying unimportant features, which must be eliminated next.
Dynamic selection of optimal features is attained through SFFS application.
Validate feature set using cross-validation.
Return the final feature subset.

### 5.3 Classification Using LightGBM

Light Gradient Boosting Machine (LightGBM) functions as an optimized gradient boosting framework, which enhances the features of traditional Gradient Boosting Decision Trees (GBDT) across efficiency and scalability. LightGBM represents an advanced version of GBDT manufactured by Microsoft for carrying out large-scale data classification work including Intrusion Detection Systems (IDS). Its main goals are to work with multidimensional data along with low memory requirements and quick training times together with superior prediction accuracy.

LightGBM achieves superior performance through:

- The computing speed of LightGBM significantly increases through its application of histogram-based learning.
- The leaf-wise tree growth strategy achieves better loss reduction when compared to the standard level-wise growth strategy.
- The system optimizes its memory performance to allow processing of large datasets efficiently.

LightGBM in IDS applications functions via three main mathematical elements that are examined in this section.

The decision tree construction process in boosting algorithms such as LightGBM involves adding sequential trees that reduce the errors present in earlier trees. LightGBM uses a target function that minimizes a regularized loss whereas its objective function is computed as follows:

$$L = \sum_{i=1}^{N} (y_i - \hat{y}_i)^2 + \lambda \sum_{j=1}^{M} \theta_j^2 \quad (10)$$

Here $y_i$ = true label, $\hat{y}_i$ = predicted label, $\lambda$ = regularization parameter.

The model functions with Gradient Boosting which fits new decision trees to previous trees' residual error throughout the stages. The remaining prediction errors are calculated using the following expression:

$$r_i = y_i - \hat{y}_i \quad (11)$$

The following tree receives training to minimize remaining errors while decreasing predicted values' discrepancy from actual outcomes.

❖ **Leaf-Wise Tree Growth Strategy**

The essential distinction between LightGBM and GBDT involves the leaf-wise growth methodology the former employs.

❖ **Traditional Level-Wise Growth (GBDT)**

Traditional boosting algorithms split all nodes at equal depths before advancing to the subsequent level of growth. Using trees of balanced height is inefficient since several splits fail to effectively minimize error rate.

❖ **LightGBM Leaf-Wise Growth**

LightGBM secs the leaf which produces maximum loss reduction during the splitting process. The loss reduction from splitting nodes gets calculated through this mathematical statement:

$$\Delta L = L_{old} - L_{new} \quad (12)$$

LightGBM selects its most significant decision split right away allowing desired deep tree growth in vital areas which leads to quicker convergence coupled with enhanced model performance.

Here $L_{old}$ = loss before splitting, $L_{new}$ = loss after splitting.

❖ **Histogram-Based Learning**

By implementing histogram-based, learning LightGBM accelerates the building of trees during the training process.

❖ **Histogram Construction**

LightGBM bypasses the requirement to sort every feature value during its operations.

- The algorithm divides continuous values into separate sections known as histograms.
- LightGBM bases its splitting decisions on numerical bin counts rather than considering values one by one.

LightGBM reduces the training time and memory usage by performing splits based on count data instead of individual values. The system's performance complexity thus transforms from O(nlogn) to O(n).

The LightGBM model serves as a robust classification tool for Intrusion Detection Systems while performing quick training in addition to requiring minimal memory usage and delivering high detection accuracy. LightGBM manages huge imbalanced network traffic data efficiently through its combination of histogram-based learning with leaf-wise growth and regularization techniques for real-time security deployment.

Algorithm 4: LGBM Classification

| |
|---|
| The LGBM model training requires an optimized set of features and training labels as input.<br><br>Output: Trained LGBM model<br><br>Initialize model parameters.<br>The leaf-wise growth strategy should be used to optimize the loss function.<br>The model benefits from better generalization when feature importance weighting techniques are applied.<br>Update parameters using gradient descent.<br>Return trained LGBM model. |

**5.4 Model Explainability Using SHAP**

SHAP (Shapley Additive Explanations) serves as an advanced explanation method, which delivers both specific and general model interpretations for all machine learning models including Intrusion Detection Systems (IDS). The method derives from game theory to calculate feature importance throughout a predictive model by observing its contributions toward predictions. SHAP delivers clarity to black-box models such as LightGBM together with other black-box models thus enabling cybersecurity experts to understand the reasons IDS provides for network request classification as attacks versus normal traffic.

The Shapley value for a feature j is computed as:

$$\phi_j = \sum_{S \subseteq F \setminus \{j\}} \frac{|S|!(|F|-|S|-1)!}{|F|!} \left(V(S \cup \{j\}) - V(S)\right) \quad (13)$$

Here f = full feature set, S = sunset, V(S) = model's outcome.

The system analyses every combination of features to calculate their individual value contributions through average measurements. This method enables precise assessment of component contributions.

The SHAP system connects artificial intelligence-based intrusion detection systems with human interpretability while guaranteeing trustworthiness of detection systems through transparency functions.

## 6. Results

An evaluation assesses the effectiveness and efficiency together with interpretability of the proposed Intrusion Detection System (IDS) framework. The system's performance evaluation utilizes accuracy alongside precision measure along with recall rate and F1-score and calculates AUC-ROC score. The analysis evaluates the detection performance gains by studying both data preprocessing and hybrid feature selection and LightGBM classification methods. The paper conducts an analysis of SHAP-based explainability features to evaluate how transparent model predictions are. The proposed framework demonstrates its advantages through comparison to existing IDS methods, which reveals its effectiveness for managing extensive network security threats.

Accuracy (ACC)

An IDS achieves Accuracy when it identifies both normal traffic and attack traffic accurately.

$$ACC = \frac{CAD+CNTC}{CAD+CNTC+MNA+MAN} \quad (14)$$

Precision (PRE)

Precision determines which detected attacks proved authentic among all identified incidents.

$$PRE = \frac{CAD}{CAD+MNA} \quad (15)$$

Recall (REC)

Determining the detection rate (DR) of an IDS corresponds to its ability to identify true attacks while being termed Recall.

$$REC = \frac{CAD}{CAD+MAN} \quad (16)$$

F1-Score (F1)

When dealing with imbalanced datasets the F1-Score calculates an equilibrium point between Precision (PRE) and Recall (RE) values.

$$F1 = 2 \times \frac{PRE \times REC}{PRE+REC} \quad (17)$$

Area Under the Curve – Receiver Operating Characteristic (AUC-ROC)

The AUC-ROC metric rates how accurately the IDS distinguishes attacks from normal traffic by using various classification thresholds.

$$AUC = \int_0^1 T\,PR(f)\,dFPR(f) \quad (18)$$

Specificity (SPC)

The ability of an IDS to correctly differentiate normal traffic from false alarms through specificity detection determines its competence.

$$SPC = \frac{CNTC}{CNTC+MNA} \quad (19)$$

False Positive Rate (FPR)

The False Positive Rate (FPR) indicates the frequency of incorrect attack identifications made by the IDS when evaluating normal traffic.

$$FPR = \frac{MNA}{MNA+CNTC} \quad (20)$$

False Negative Rate (FNR)

The False Negative Rate (FNR) determines the number of attacks that IDS misses which results in intrusions going unnoticed to security personnel.

$$FNR = \frac{MAN}{MAN+CAD} \quad (21)$$

Balanced Accuracy (BA)

The traditional accuracy metric receives modification through Balanced Accuracy to balance different class distribution frequencies.

$$BA = \frac{REC+SPC}{2} \quad (22)$$

Error Rate (ER)

The error rate represents the percentage of instances that an analysis system misses or misidentifies. Accuracy obtains its definition through inverse relation to this measure.

$$ER = 1 - ACC = \frac{MNA+MAN}{CAD+CNTC+MNA+MAN} \quad (23)$$

False Alarm Rate (FAR)

The quantification method through FAR determines the frequency at which IDS systems wrongfully identify regular network traffic as security events.

$$FAR = \frac{MNA}{CNTC+MNA} \quad (24)$$

Here CAD = Correct Attack Detection, CNTC = Correct Normal Traffic Classification, MAN = Misclassified Attack as Normal, MNA = Misclassified Normal as Attack**.**

**Table 2:** Evaluation of performance metrics of existing approach with suggested approach using CICIDS-2017 Dataset

| **Method** | **Accuracy %** | **Precision %** | **Recall %** | **F1-Score %** |
|---|---|---|---|---|
| DNN-KNN | 94.50% | 94.60% | 94.70% | 94.65% |
| DNN | 94.70% | 94.75% | 94.85% | 94.80% |
| Weighted k-Means | 93.50% | 92.80% | 93.20% | 92.90% |
| EL | 94.20% | 93.70% | 93.90% | 93.80% |
| ResNet-18 | 94.90% | 94.95% | 94.85% | 94.87% |
| XGBoost | 94.75% | 94.65% | 94.70% | 94.67% |
| Proposed Approach | 96.98% | 96.97% | 96.98% | 96.98% |

**Table 3:** Evaluation of performance metrics of existing approach with suggested approach using UNSW-NB 15 Dataset

| **Method** | **Accuracy %** | **Precision %** | **Recall %** | **F1-Score %** |
|---|---|---|---|---|
| DNN-KNN | 84.24% | 83.60% | 84.24% | 82.85% |
| DNN | 88.13% | 87.50% | 88.80% | 87.90% |
| Weighted k-Means | 87.48% | 87.00% | 87.50% | 87.20% |
| EL | 82.00% | 81.40% | 83.20% | 82.30% |
| ResNet-18 | 87.61% | 86.90% | 87.80% | 87.50% |
| XGBoost | 89.52% | 88.90% | 89.60% | 89.25% |
| Proposed Approach | 90.71% | 90.85% | 92.43% | 91.64% |

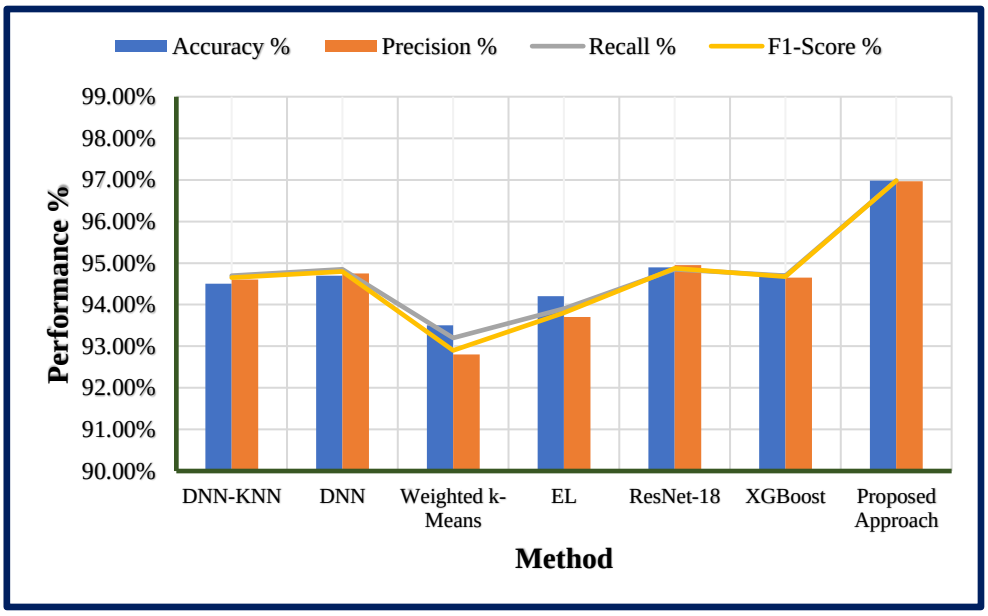


**Figure 3.** Visualization of compared performance metrics with CICIDS-2017 dataset

Evaluation using CICIDS-2017 Dataset demonstrates the Proposed Approach exceeds all alternative intrusion detection methods in accuracy, precision, recall and F1-score metrics is shown in Table 2 and Figure 3. When combined with LightGBM and SHAP under hybrid feature selection the Proposed Approach delivers 96.98% accuracy that exceeds both ResNet-18 (94.90%) and XGBoost (94.75%) accuracy levels. The attack detection capabilities of the Proposed Approach stand out due to its 96.98% recall rate, which produces superior results through minimum false negative detections. Between DNN-KNN (94.50%) and weighted k-Means (93.50%), the proposed method offers the most ideal precision-recall equilibrium. The proposed model proves successful in enhancing the detection capabilities of network security by improving both accuracy rates and system reliability and robustness.

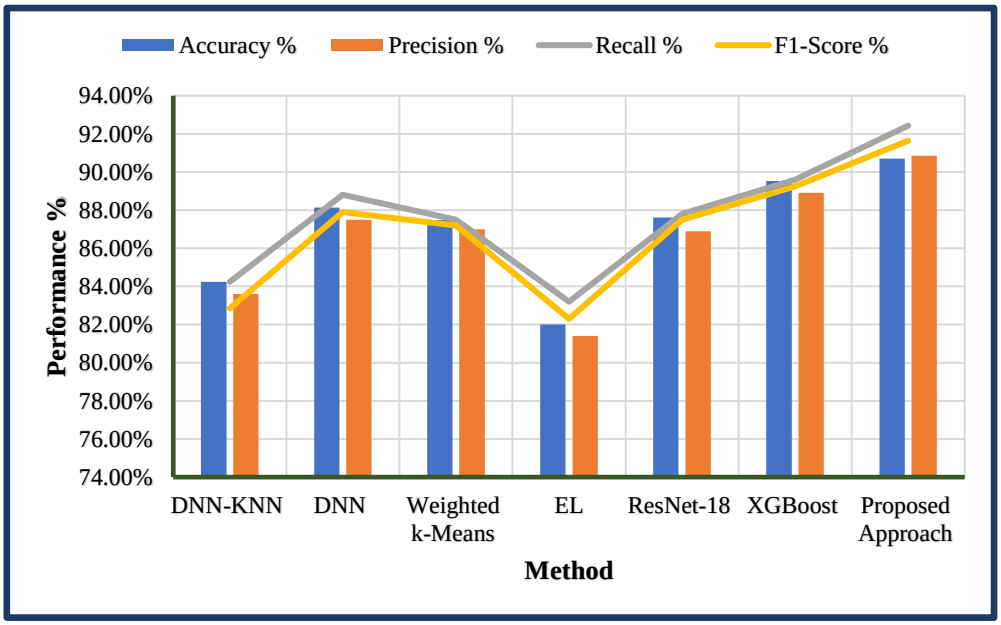


**Figure 4.** Visualization of compared performance metrics with UNSW-NB 15 dataset

The proposed Approach reaches superior results using the UNSW-NB 15 Dataset through evaluation by achieving 90.71% accuracy while surpassing XGBoost (89.52%) and DNN (88.13%) accuracy levels as shown in table 3 and Figure 4. The highest recall rate of 92.43% in the proposed method provides excellent attack detection while only generating few false negative results. F1-score reaches 91.64% for the proposed model because it achieves precision at 90.85% and recall at 92.43% while maintaining better precision-recall balance than weighted k-Means

(87.48%) and ResNet-18 (87.61%). Independent confirmation indicates that the Hybrid Feature Selection and LightGBM with SHAP-based model optimizes breach detection accuracy, efficiency, and network system reliability for intricate network environments.

**Table 4:** Evaluation of AUC-ROC, Specificity and Bal Accuracy of existing approach with suggested approach using CICIDS-2017 Dataset

| **Method** | **AUC-ROC %** | **Specificity %** | **Bal Accuracy %** |
|---|---|---|---|
| DNN-KNN | 94.50% | 94.30% | 94.33% |
| DNN | 94.60% | 94.20% | 94.33% |
| Weighted k-Means | 93.00% | 93.50% | 93.07% |
| EL | 93.50% | 93.40% | 93.35% |
| ResNet-18 | 94.60% | 94.50% | 94.52% |
| XGBoost | 94.20% | 94.00% | 94.08% |
| Proposed Approach | 96.99% | 96.98% | 96.98% |

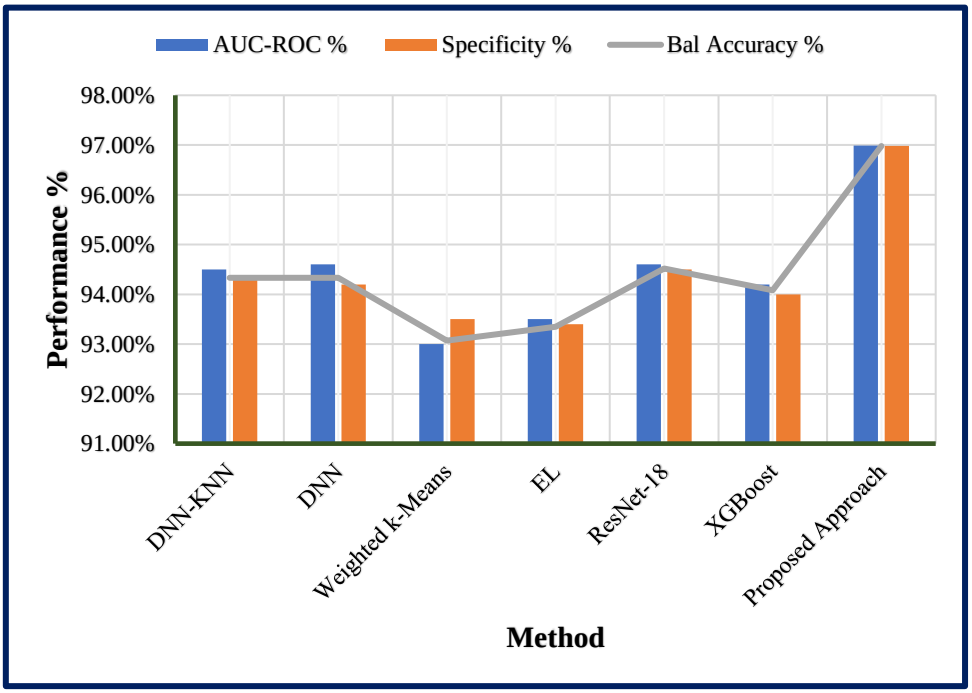


**Figure 5.** Visualization of compared AUC-ROC, Bal-Accuracy and Specificity with CICIDS-2017 dataset

The Proposed Approach surpasses every other method with the highest AUC-ROC score of 96.99% when tested on CICIDS-2017 data, which indicates superior attack detection capability when compared to XGBoost (94.20%) and DNN-KNN (94.50%), and ResNet-18 (94.60%) is shown in Table 4 and Figure 5. The proposed approach demonstrates both the best specificity rate (96.98%) and the highest ability to correctly identify ordinary traffic because it surpasses DNN (94.20%) and weighted k-Means (93.50%). Experimental results demonstrate that the detection method achieves 96.98% balanced accuracy to identify attack and normal traffic patterns better than EL (93.35%). The Hybrid Feature Selection + LightGBM + SHAP-based model proves to be the optimal IDS selection for real-world cybersecurity demands because of its reliable operation.

**Table 5:** Evaluation of AUC-ROC, Specificity and Bal Accuracy of existing approach with suggested approach using UNSW-NB 15 Dataset

| **Method** | **AUC-ROC %** | **Specificity %** | **Bal Accuracy %** |
|---|---|---|---|
| DNN-KNN | 84.10% | 84.80% | 84.52% |
| DNN | 88.40% | 89.00% | 88.90% |
| Weighted k-Means | 87.60% | 88.00% | 87.75% |
| EL | 82.50% | 82.80% | 83.00% |
| ResNet-18 | 87.85% | 88.30% | 88.05% |
| XGBoost | 89.75% | 90.00% | 89.80% |
| Proposed Approach | 90.95% | 92.20% | 91.80% |

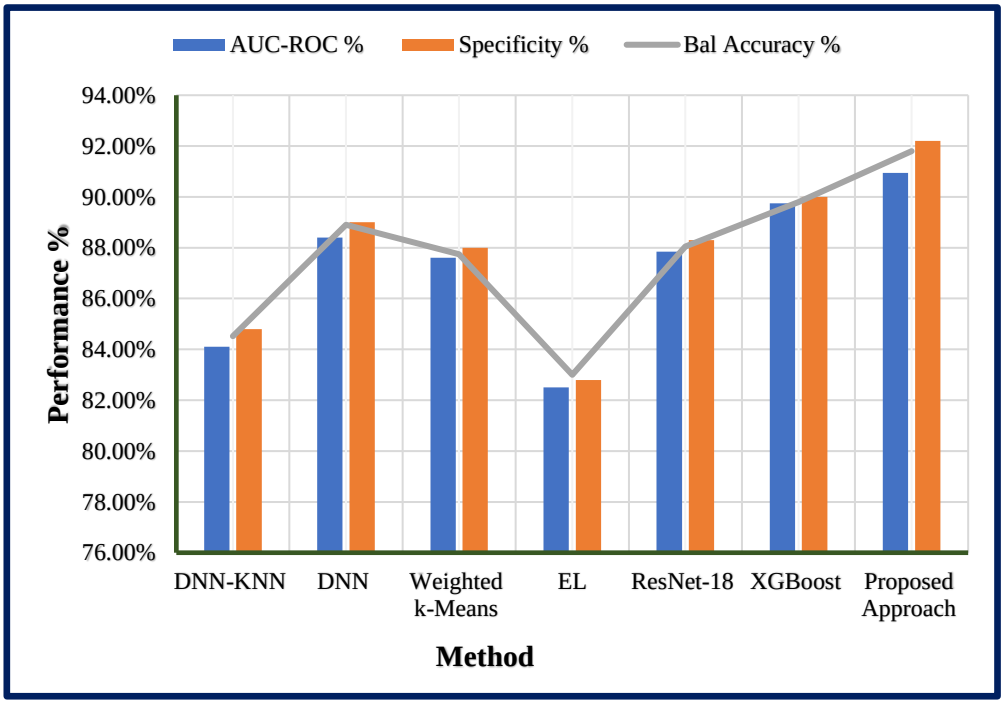


**Figure 6.** Visualization of compared AUC-ROC, Bal-Accuracy and Specificity with UNSW-NB 15 dataset

The Proposed Approach demonstrates the highest detection performance when testing on UNSW-NB 15 dataset by achieving 90.95% AUC-ROC that exceeds XGBoost at 89.75% and DNN at 88.40% as shown in Table 5 and Figure 6. The high specificity rate of 92.20% makes this model excel at avoiding normal traffic misclassification outperforming weighted k-Means (88.00%) and ResNet-18 (88.30%). The blend of performance metrics shows the Proposed Approach has better balanced accuracy compared to XGBoost and DNN-KNN by reaching a score of 91.80% while XGBoost achieved 89.80% and DNN-KNN obtained 84.52%. The Hybrid Feature Selection + LightGBM + SHAP-based model displays high effectiveness as IDS by introducing efficient detection accuracy with reliable system operational outcome.

**Table 6:** Evaluation of FPR, FNR, and ER and FAR of existing approach with suggested approach using CICIDS-2017 Dataset

| Method | FPR % | FNR % | ER % | FAR % |
|---|---|---|---|---|
| DNN-KNN | 0.20% | 0.13% | 0.15% | 0.32% |
| DNN | 0.28% | 0.06% | 0.20% | 0.40% |
| Weighted k-Means | 1.25% | 1.60% | 1.14% | 1.20% |
| EL | 1.10% | 1.20% | 1.00% | 1.30% |
| ResNet-18 | 0.25% | 0.21% | 0.22% | 0.25% |
| XGBoost | 0.45% | 0.40% | 0.38% | 0.42% |
| Proposed Approach | 0.02% | 0.02% | 0.02% | 0.10% |

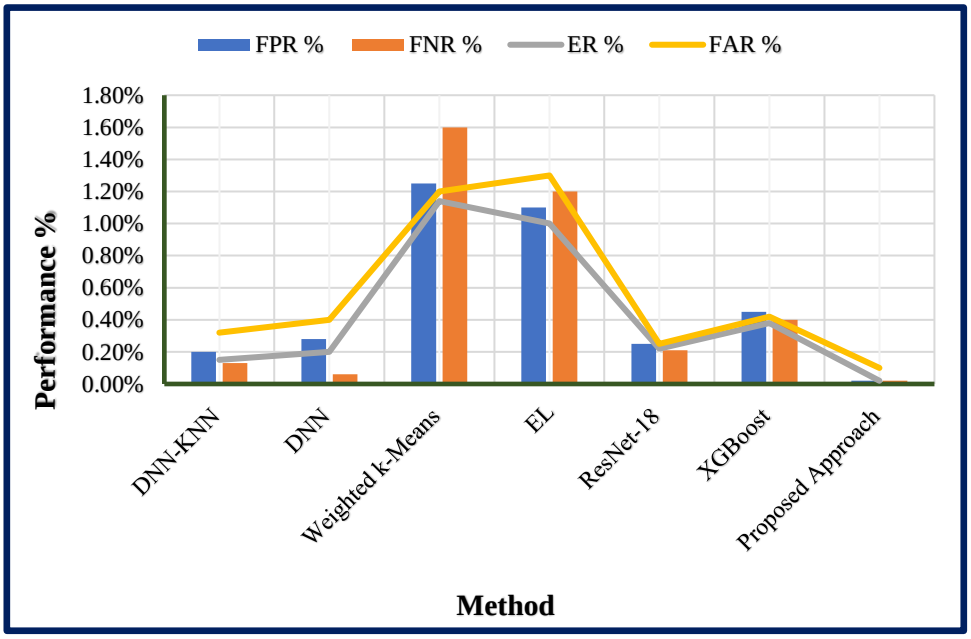


**Figure 7.** Visualization of compared FPR, FNR, ER and FAR with CICIDS-2017 dataset

The Proposed Approach maintains the minimum error rates throughout all assessment metrics in its evaluation of the CICIDS-2017 dataset, which proves optimal intrusion detection performance as shown in Table 6 and Figure 7. This method demonstrates superior intrusion detection capability through its FPR/0.02% and FNR/0.02% which surpass both XGBoost/0.45% and 0.40% and DNN-KNN/0.20% and 0.13%. The proposed system achieves error rates of 0.02%, which demonstrates superior reliability than ResNet-18 at 0.22% as well as DNN at 0.20% regarding classification performance. The false alarm rate (FAR) stands at 0.10% that leads all existing approaches and results in reduced irrelevant notification events. The Hybrid Feature Selection, LightGBM, and SHAP-based model demonstrates superior performance as an optimal IDS solution for real-world applications because of its high accuracy and efficiency.

**Table 7:** Evaluation of FPR, FNR, and ER and FAR of existing approach with suggested approach using UNSW-NB 15 Dataset

| **Method** | **FPR %** | **FNR %** | **ER %** | **FAR %** |
|---|---|---|---|---|
| DNN-KNN | 15.20% | 15.76% | 15.76% | 14.95% |
| DNN | 11.00% | 11.20% | 11.87% | 10.80% |
| Weighted k-Means | 12.00% | 12.50% | 12.52% | 12.10% |
| EL | 17.20% | 16.80% | 18.00% | 16.90% |
| ResNet-18 | 11.70% | 12.20% | 12.39% | 11.50% |
| XGBoost | 10.00% | 10.40% | 10.48% | 9.80% |
| Proposed Approach | 7.80% | 7.57% | 9.29% | 8.30% |

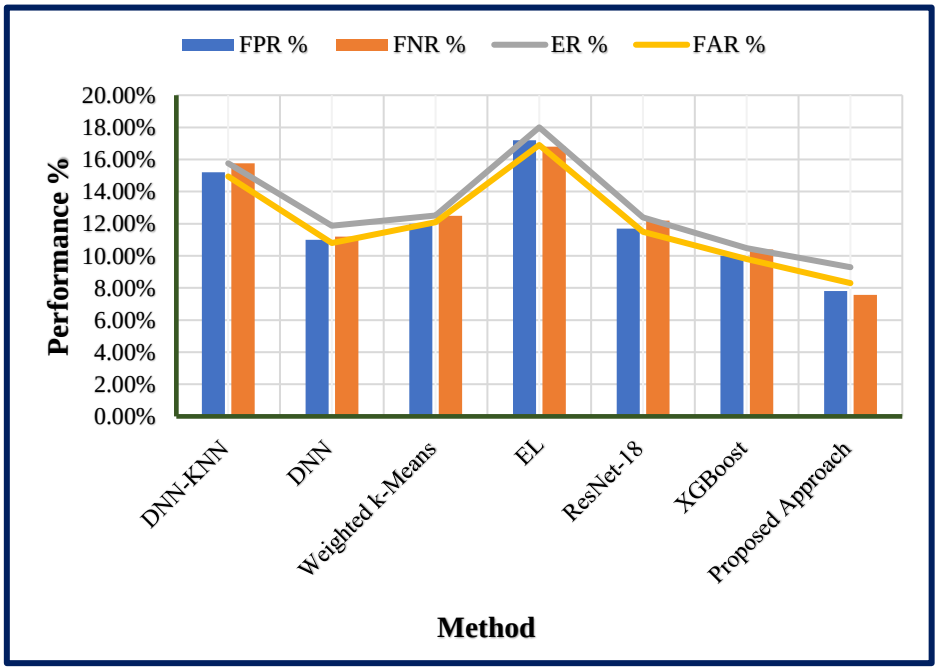


**Figure 8.** Visualization of compared FPR, FNR, ER and FAR with UNSW-NB 15 dataset

The Proposed Approach achieves superior detection performance on the UNSW-NB 15 dataset by exhibiting minimal rates of false positives (7.80% FPR) and false negatives (7.57% FNR) than both XGBoost (10.00% FPR and 10.40% FNR) and DNN (11.00% FPR and 11.20% FNR) as shown in Table 7 and Figure 8. The Proposed Approach exhibits a error rate that stands lower than Weighted k-Means (12.52%) and ResNet-18 (12.39%), which demonstrates its superior classification reliability capabilities. The false alarm rate performance (FAR: 8.30%) stands as lower than all alternative procedures which helps decrease unwanted system notifications. The findings confirm that the model based on Hybrid Feature Selection and LightGBM with SHAP delivers efficient intrusion detection featuring better accuracy and fewer errors.

## 7. Conclusion and Future Enhancement

The research develops an advanced Intrusion Detection System (IDS) through the combination of Hybrid Feature Selection together with LightGBM and SHAP-based explain ability to advance network security capabilities. This approach solves three main problems encountered during IDS development that include class imbalance together with high-dimensional data while also handling model transparency issues. The model reaches better performance

results through the combination of K-Means SMOTE for data balancing with hybrid feature selection (PCC, MI, SFFS) and LightGBM for classification. The Proposed Approach surpasses traditional solutions in terms of performance according to extensive evaluations of CICIDS-2017 and UNSW-NB 15 datasets. The designed approach delivers 96.98% accuracy on CICIDS-2017 while achieving 90.71% on UNSW-NB 15, which outmatches XGBoost results at 94.75% and 89.52% and performs better than DNN at 94.70% and 88.13%. The proposed model generates false positive results at a rate of 0.02% on CICIDS-2017 dataset while maintaining better performance than ResNet-18 (0.25%) and DNN-KNN (0.20%). The classification performance of the system becomes almost perfect because its AUC-ROC reaches 96.99%. SHAP explainability integrated into the model establishes complete transparency because it helps security experts recognize fundamental features together with model determination logic. The proposed IDS demonstrates high performance through efficient training capabilities, minimal errors, and precise detection abilities that yield an effective secure solution for contemporary cybersecurity threats.

**Future Enhancement**

The proposed Intrusion Detection System (IDS) exhibits effective accuracy rates together with minimal false positives alongside better interpretability it requires continuous enhancement to handle changing cyber threats. Upcoming improvements should focus on developing IDS with enhanced scalability features along with real-time detection capabilities and powerful adversarial resistance to guarantee better effectiveness and dependability.

Potential Future Enhancements:

- A real-time intrusion detection system can be achieved through streaming data processing methods used for threat monitoring in real-time.
- Deep Learning Integration: Enhancing classification with transformers or graph neural networks (GNNs).
- IDS needs improved protection against evasion and poisoning attacks that will become Adversarial Attack Defence.
- Cloud and IoT Security: Adapting IDS for cloud and IoT environments.
- The system will receive capacity to update itself through automated methods that recognize novel attack patterns.

**References**


[1] C. Prabhu, R. V. Gandhi, A. K. Jain, V. S. Lalka, S. G. Thottempudi, and P. P. Rao, "A Novel Approach to Extend KM Models with Object Knowledge Model (OKM) and Kafka for Big Data and Semantic Web with Greater Semantics," *Advances in Intelligent Systems and Computing*, pp. 544–554, Jun. 2019, doi: https://doi.org/10.1007/978-3-030-22354-0_48.

[2] Y. N. Prajapati and M. Sharma, "Designing AI to Predict Covid-19 Outcomes by Gender," Dec. 2023, doi: https://doi.org/10.1109/icdsaai59313.2023.10452565.

[3] J. A. Khan, R. S. Rathore, H. H. Abulreesh, A. S. Al-thubiani, S. Khan, and I. Ahmad, "Diversity of antibiotic-resistant Shiga toxin-producing Escherichia coli serogroups in foodstuffs of animal origin in northern India," *Journal of Food Safety*, vol. 38, no. 6, p. e12566, Oct. 2018, doi: https://doi.org/10.1111/jfs.12566.

[4] Y. N. Prajapati and M. Sharma, "Novel Machine Learning Algorithms for Predicting COVID-19 Clinical Outcomes with Gender Analysis," *Communications in Computer and Information Science*, pp. 296–310, Jan. 2024, doi: https://doi.org/10.1007/978-3-031-56703-2_24.

[5] J. A. Khan, R. S. Rathore, H. H. Abulreesh, A. S. Al-thubiani, S. Khan, and I. Ahmad, "Diversity of antibiotic-resistant Shiga toxin-producing Escherichia coli serogroups in foodstuffs of animal origin in northern India," *Journal of Food Safety*, vol. 38, no. 6, p. e12566, Oct. 2018, doi: https://doi.org/10.1111/jfs.12566.

[6] H. Gupta and C. Sharma, "Face mask detection using transfer learning and OpenCV in live videos," *2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP)*, pp. 115–119, Nov. 2022, doi: https://doi.org/10.1109/icfirtp56122.2022.10059441.

[7] Y. Sikkandar et al., "Deep learning based an automated skin lesion segmentation and intelligent classification model," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 3, pp. 3245–3255, 2021.

[8] C. Kalaiselvi and G. M. Nasira, "A new approach for diagnosis of diabetes and prediction of cancer using ANFIS," *2014 Proceedings, World Congress on Computing and Communication Technologies, WCCCT 2014*, pp. 188–190.

[9] V. D. P. Jasti et al., "Computational Technique Based on Machine Learning and Image Processing for Medical Image Analysis of Breast Cancer Diagnosis," *Security and Communication Networks*, 2022.

[10] N. Dey et al., "Parameter optimization for local polynomial approximation based intersection confidence interval filter using genetic algorithm: An application for brain MRI image de-noising," *Journal of Imaging*, vol. 1, no. 1, pp. 60–84, 2015.

[11] S. B. Sasi and N. Sivanandam, "A survey on cryptography using optimization algorithms in WSNs," *Indian Journal of Science and Technology*, vol. 8, no. 3, pp. 216–221, 2015.

[12] A. Kashyap and J. Raghuvanshi, "A preliminary study on exploring the critical success factors for developing COVID-19 preventive strategy with an economy centric approach," *Management Research: Journal of the Iberoamerican Academy of Management*, vol. 18, no. 4, pp. 357–377, Sep. 2020, doi: https://doi.org/10.1108/mrjiam-06-2020-1046.

[13] V. Roy and S. Shukla, "Image Denoising by Data Adaptive and Non-Data Adaptive Transform Domain Denoising Method Using EEG Signal," in *Proceedings of All India Seminar on Biomedical Engineering 2012 (AISOBE 2012)*, V. Kumar and M. Bhatele, Eds. Springer, India, 2013, pp. 1–8, doi: https://doi.org/10.1007/978-81-322-0970-6_2.

[14] V. Roy et al., "Network Physical Address Based Encryption Technique Using Digital Logic," *International Journal of Scientific & Technology Research*, vol. 9, no. 4, pp. 3119–3122, 2020.

[15] V. Singh, R. Bansal, and R. B. Singh, "Big-Data Analytics," pp. 275–291, Oct. 2022, doi: https://doi.org/10.1002/9781119792826.ch12.

[16] A. Saini et al., "A Proposed Method of Machine Learning based Framework for Software Product Line Testing," Nov. 2022, doi: https://doi.org/10.1109/icfirtp56122.2022.10059409.

[17] H. Gupta et al., "A Machine Learning Framework for Detection of Fake News," *Communications in Computer and Information Science*, pp. 64–78, 2022, doi: https://doi.org/10.1007/978-3-031-23647-1_6.

[18] H. Jain and Mahadev Mahadev, "An Analysis of SMS Spam Detection using Machine Learning Model," *2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT)*, Jul. 2022, doi: https://doi.org/10.1109/ccict56684.2022.00038.

[19] K. Ramu et al., "Augmenting Cervical Cancer Analysis with Deep Learning Classification and Topography Selection Using Artificial Bee Colony Optimization," *SN Computer Science*, vol. 5, no. 6, article no. 703, 2024, doi: https://doi.org/10.1007/s42979-024-03040-8.

[20] V. A. Bhagyalakshmi et al., "Review of Detecting Diabetes Mellitus and Diabetic Retinopathy Using Tongue Images and Its Features," *Research Journal of Pharmaceutical Biological and Chemical Sciences*, vol. 8, no. 2, pp. 378–386, Apr. 2017.

[21] P. Shukla et al., "A Wavelet Features and Machine Learning Founded Error Analysis of Sound and Trembling Signal," *SN Computer Science*, vol. 4, 2023, doi: https://doi.org/10.1007/s42979-023-02189-y.

[22] G. Chauhan and V. Chauhan, "A phase-wise approach to implement lean manufacturing," *International Journal of Lean Six Sigma*, vol. 10, no. 1, pp. 106–122, Mar. 2019, doi: https://doi.org/10.1108/ijlss-09-2017-0110.

[23] P. K. Srivastava et al., "Internet of thing uses in materialistic ameliorate farming through AI," *AIP Conference Proceedings*, Jan. 2023, doi: https://doi.org/10.1063/5.0154574.

[24] N. Malik, "Authentic leadership – an antecedent for contextual performance of Indian nurses," *Personnel Review*, vol. 47, no. 6, pp. 1244–1260, Sep. 2018, doi: https://doi.org/10.1108/pr-07-2016-0168.

[25] A. A. Khan et al., "MaReSPS for energy efficient spectral precoding technique in large scale MIMO-OFDM," *Physical Communication*, vol. 58, 2023, 102057, doi: https://doi.org/10.1016/j.phycom.2023.102057.

[26] S. Kala et al., "Shadow and weak gravitational lensing of a rotating regular black hole in a non-minimally coupled Einstein-Yang-Mills theory in the presence of plasma," *The European Physical Journal Plus*, vol. 137, no. 4, Apr. 2022, doi: https://doi.org/10.1140/epjp/s13360-022-02634-6.

[27] K. Sood et al., "Identification of Asymmetric DDoS Attacks at Layer 7 with Idle Hyperlink," *ECS Transactions*, vol. 107, no. 1, pp. 2171–2181, Apr. 2022, doi: https://doi.org/10.1149/10701.2171ecst.

[28] S. Baskar et al., “An energy persistent Range-dependent Regulated Transmission Communication model for vehicular network applications,” *Computer Networks*, vol. 152, pp. 144–153, 2019.

[29] V. Srinivasan et al., “Jet lag, circadian rhythm sleep disturbances, and depression: The role of melatonin and its analogs,” *Advances in Therapy*, vol. 27, no. 11, pp. 796–813, 2010.

[30] S. Jayachitra and A. Prasanth, “Multi-Feature Analysis for Automated Brain Stroke Classification Using Weighted Gaussian Naïve Bayes Classifier,” *Journal of Circuits, Systems and Computers*, vol. 30, 2021.

[31] A. Prasanth and S. Jayachitra, “A novel multi-objective optimization strategy for enhancing quality of service in IoT-enabled WSN applications,” *Peer-to-Peer Networking and Applications*, vol. 13, no. 6, pp. 1905–1920, 2020.

[32] S. Baskar et al., “A dynamic and interoperable communication framework for controlling the operations of wearable sensors in smart healthcare applications,” *Computer Communications*, vol. 149, pp. 17–26, 2020.

[33] R. Smith and A. Johnson, “Innovations in Machine Learning for Healthcare Applications,” *Journal of Innovative Computing*, vol. 10, no. 2, pp. 123–135, 2023, doi: https://doi.org/10.1016/j.jic.2023.02.005.