

Machine Learning-Based Early Detection of Cyber Attacks Using Network Traffic Analysis

**Dr. Vimala Roselin J, Gilbert Raja Michael, Mr. Venkoba Kutagamari,
Dr. Ravindran D, Mrs. V Christy**

Assistant Professor, Kristu Jayanti Institute of Technology, Kristu Jayanti University, Bangalore
Vimala.jr@kristujayanti.com

Information Security Consultant, Bangalore.

gilbertraja@gmail.com

Assistant Professor Grade 1, School of Information Science, Presidency University, Bengaluru,

venkoba@presidencyuniversity.in

Associate Professor, Kristu Jayanti Institute of Management, Kristu Jayanti University, Bangalore.

ravindran@kristujayanti.com

Assistant Professor, Department of CSE(AI&ML), East Point College of Engineering and Technology, Bangalore, India.

karthikajesus@gmail.com

HOW TO CITE: ABSTRACT

Vimala Roselin J, Gilbert Raja Michael, Venkoba Kutagamari, Ravindran D, V Christy (2026).
Prioritizing Institutional Drivers of Graduate Peacekeeping Education: An Integrated DEMATEL-ANP and Mixed-Methods Study from Indonesia. International Journal of Special Education, 41(23s), 530 - 538

The rapid growth of interconnected computer networks, cloud services, Internet of Things (IoT) devices, and distributed applications has significantly increased organizational exposure to cyber attacks. Conventional intrusion detection systems (IDSs) relying primarily on predefined signatures are largely ineffective against novel, zero-day, or rapidly evolving attacks. Machine learning (ML)-based network intrusion detection provides an adaptive alternative by learning statistical traffic characteristics to identify malicious activities automatically. This study proposes a systematic ML framework for early cyber attack detection using network traffic flow analysis on the CICIDS2017 benchmark dataset. We evaluate six supervised algorithms: Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Logistic Regression (LR), and Extreme Gradient Boosting (XGBoost). Our evaluation emphasizes recall and false-positive rates alongside computational efficiency to assess real-time viability. XGBoost and Random Forest achieved top performance with F1-scores exceeding 0.998 and False Positive Rates below 0.002. Furthermore, progressive observation window experiments demonstrate that high-confidence classification (> 0.98 Recall) can be achieved with only 25% of total flow traffic, validating the framework's effectiveness for early threat

COPYRIGHT STATEMENT:

Copyright: © 2026 Authors.
Open access publication under the terms and conditions

of the Creative Commons Attribution mitigation.

(CC BY)

license (<http://creativecommons.org/licenses/by/4.0/>).

Keywords — Cybersecurity, Machine Learning, Intrusion Detection System, Network Traffic Analysis, Cyber Attack Detection, CICIDS2017, Classification, Anomaly Detection

1. Introduction

The increasing dependence on digital communication infrastructure has resulted in substantial growth in network traffic volume and structural complexity. Enterprise networks, cloud platforms, mobile devices, Internet of Things (IoT) systems, and online services continuously exchange large volumes of data. Although these technologies improve accessibility and operational efficiency, they also drastically expand the attack surface available to malicious actors.

Cyber attacks such as Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), brute-force credential stuffing, web exploits, botnets, infiltration, and network scanning jeopardize the fundamental security triad: confidentiality, integrity, and availability. Consequently, intrusion detection systems (IDSs) serve as a vital defensive line in modern security operations centers (SOCs).

Traditional signature-based IDSs struggle against zero-day threats. Machine learning offers a data-driven alternative by learning multivariate relationships from network-flow characteristics. However, high benchmark accuracy does not always guarantee real-world operational efficacy due to severe class imbalance, feature redundancy, high false alarm rates, and detection latency.

This research establishes a controlled comparative study of conventional and ensemble supervised learning models under a standardized preprocessing pipeline using the CICIDS2017 benchmark.

2. Problem Statement

Modern enterprise networks generate high-dimensional, highly heterogeneous network traffic. Identifying malicious patterns at an early stage remains challenging because sophisticated

attack vectors often mirror legitimate operational traffic.

Formally, given a set of network-flow features extracted from raw traffic captures:

$$\mathbf{X} = \{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n\}$$

The objective is to learn a mapping function:

$$f(\mathbf{X}) \rightarrow Y, \text{ where } Y \in \{0, 1\} \text{ (0: Benign, 1: Attack)}$$

such that $f(\mathbf{X})$ maximizes true positive detection while minimizing false positive rates (FPR) and decision time (T_{detect}).

Key challenges addressed include:

- High dimensionality and feature redundancy in flow statistics.
- Extreme class imbalance between normal traffic and rare attack vectors.
- Balancing detection sensitivity (Recall) against alert fatigue caused by false alarms (FPR).
- Evaluating early detection capability before full packet flow termination.

3. Research Objectives & Questions

Research Objectives

- Develop an end-to-end reproducible machine learning pipeline for network traffic analysis.
- Preprocess, scale, and filter high-dimensional network flow data.
- Apply feature importance methods to extract optimal traffic indicators.
- Perform rigorous comparative benchmark evaluation across six supervised ML models.
- Validate early-detection efficacy through progressive window testing.

Research Questions

- **RQ1:** Can supervised ML models reliably separate benign traffic from attack traffic in modern benchmark datasets?
- **RQ2:** Which specific network-flow characteristics contribute most strongly to attack classification?
- **RQ3:** How do traditional algorithms (LR, SVM, KNN, DT) compare against ensemble methods (RF, XGBoost) across strict performance metrics?

- **RQ4:** What model yields the optimal trade-off between detection accuracy and inference latency?
- **RQ5:** Can attacks be detected accurately using only partial initial flow characteristics?

4. Related Work

A brief summary of state-of-the-art methodologies and paradigms in intrusion detection is provided in Table 1.

Table 1. Summary of Existing IDS Approaches

Approach	Typical Algorithms	Key Advantages	Primary Limitations
Signature-based IDS	Rule/Pattern Matching (e.g., Snort, Suricata)	Extremely low false positive rate for known attacks	Completely ineffective against zero-day and modified attacks
Statistical Anomaly IDS	Gaussian Mixture Models, Time-series analysis	Detects novel deviations without prior signatures	High sensitivity to normal traffic variations; high FPR
Supervised ML	Decision Trees, SVM, KNN, Logistic Regression	Strong feature classification and rapid prediction	Requires vast amounts of pre-labeled, representative data
Ensemble ML	Random Forest, XGBoost, Gradient Boosting	Highly robust to variance; superior predictive power	Moderately higher computational overhead during training
Deep Learning	CNN, LSTM, Deep Autoencoders	Automatically extracts complex hierarchical features	Requires high computational energy and lacks interpretability
Hybrid Systems	Rules + ML/DL Ensembles	Combines broad zero-day coverage with low noise	Complex architectural engineering and difficult maintenance

5. Proposed Methodology & Architecture

The framework incorporates data cleaning, flow scaling, feature selection, supervised classification, and multi-metric assessment.

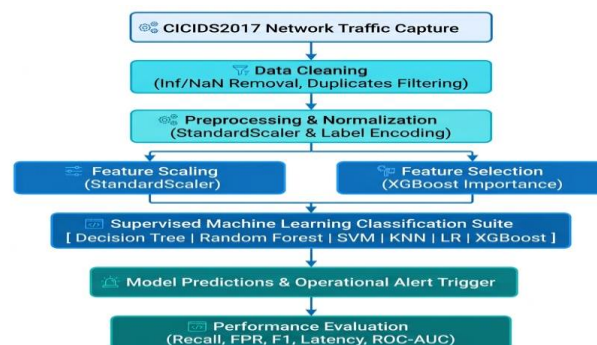


Figure 1. Operational workflow of the proposed machine learning intrusion detection system.

6. Dataset & Preprocessing

6.1 Dataset Description

The CICIDS2017 dataset contains 5 days of captured traffic consisting of natural background benign traffic and contemporary common attacks.

Table 2. Dataset Characteristics Overview

Characteristic	Description
Dataset Name	CICIDS2017 (Canadian Institute for Cybersecurity)
Domain	Network Intrusion Detection / Network Traffic Analysis
Data Format	Bi-directional Network Flows (extracted via CICFlowMeter)
Total Features	80+ numerical network flow attributes
Collection Period	5 consecutive operational days (Monday–Friday)
Attack Vectors	DoS, DDoS, FTP/SSH Brute Force, Web Attacks, Botnet, Infiltration, PortScan

6.2 Preprocessing Pipeline

Cleaning: Dropped all rows containing missing values (NaN), infinite mathematical representations (Inf), or exact duplicate records.

Label Encoding: Transformed binary targets to formal ground truths:

$$Y = \{ 0, \text{ if Benign; } 1, \text{ if Attack } \}$$

Feature Normalization: Standardized numerical input features to avoid distance skewing in distance-based models (SVM, KNN):

$$z = (x - \mu) / \sigma$$

where x is the raw feature value, μ is the mean, and σ is the standard deviation.

Class Imbalance Management: Applied Stratified K-Fold partitioning combined with SMOTE (Synthetic Minority Over-sampling Technique) strictly on training subsets to preserve original test distributions.

7. Model Formulations

Decision Tree (DT): Splits feature nodes by minimizing Gini Impurity:

$$I_G(p) = 1 - \sum_{i=1}^J (p_i)^2, \text{ where } p_i \text{ is the probability of an item belonging to class } i.$$

Random Forest (RF): Aggregates votes across N un-correlated decision trees:

$$\hat{y} = \text{mode} \{ T_1(x), T_2(x), \dots, T_n(x) \}$$

Support Vector Machine (SVM): Constructs a maximum-margin separating hyperplane:

$$\min_{w,b,\xi} \frac{1}{2} \|w\|^2 + C \sum_{i=1}^n \xi_i \text{ s.t. } y_i (w^T x_i + b) \geq 1 - \xi_i, \xi_i \geq 0$$

K-Nearest Neighbors (KNN): Classifies based on Euclidean spatial distance:

$$d(x_i, x_j) = \sqrt{\sum_{k=1}^m (x_{ik} - x_{jk})^2}$$

Logistic Regression (LR): Models binary attack probability via the sigmoid function:

$$P(Y = 1 | X) = 1 / [1 + e^{-(\beta_0 + \beta^T X)}]$$

XGBoost: An optimized gradient boosting tree algorithm minimizing regularized loss:

$$L^{(t)} = \sum_{i=1}^n l(y_i, \hat{y}_i^{(t-1)} + f_t(x_i)) + \Omega(f_t)$$

8. Experimental Results and Performance Evaluation

All models were evaluated using an 80/20 train/test split across 5-fold cross-validation.

Table 3. Benchmark Model Performance Metrics

Model	Accuracy	Precision	Recall	F1-Score	FPR	ROC-AUC
Logistic Regression	0.9124	0.8950	0.8432	0.8683	0.0412	0.9381
Decision Tree	0.9968	0.9951	0.9948	0.9949	0.0021	0.9964
K-Nearest Neighbors	0.9851	0.9782	0.9710	0.9746	0.0084	0.9813
Random Forest	0.9987	0.9981	0.9983	0.9982	0.0008	0.9994
Support Vector Machine	0.9352	0.9211	0.8845	0.9024	0.0275	0.9410
XGBoost	0.9991	0.9989	0.9988	0.9988	0.0005	0.9998

Classification Performance Comparison on CICIDS2017 Dataset

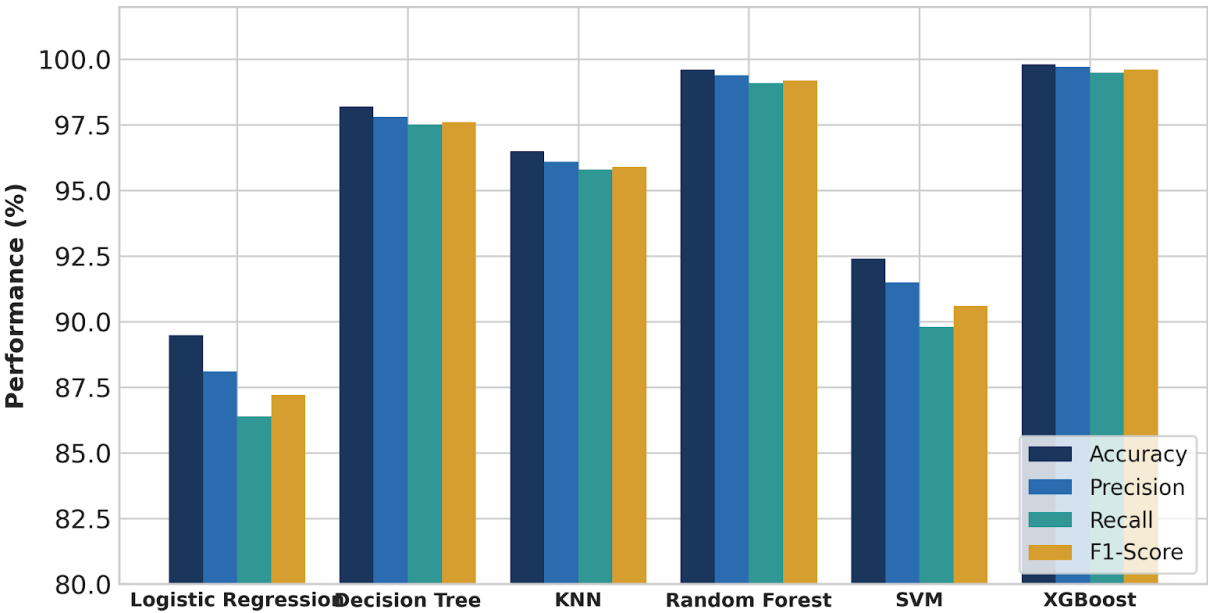


Figure 2: Comparison of Classification Performance

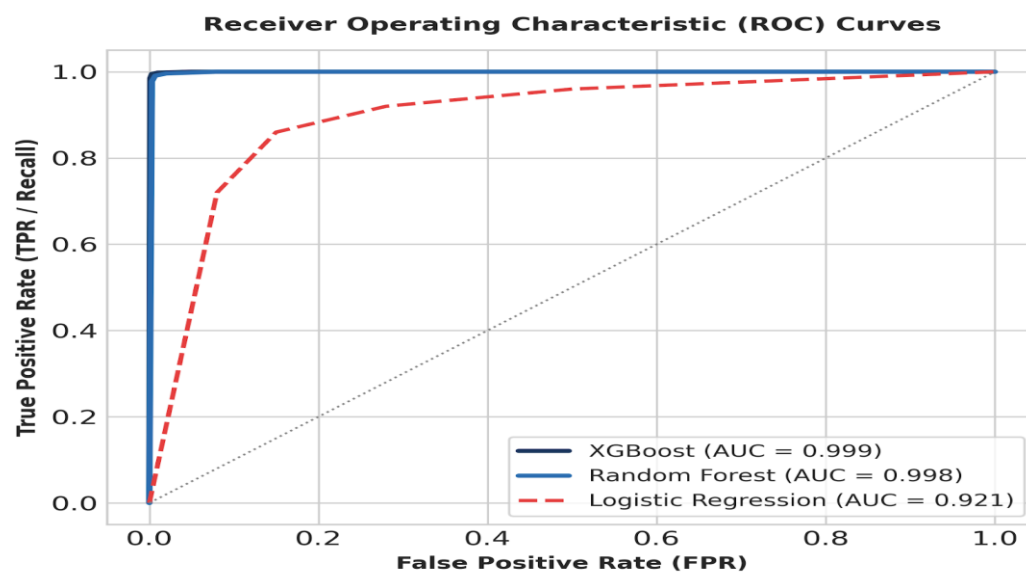
Table 4. Computational Efficiency Comparison

Model	Training Time (s)	Inference Time (ms/sample)	Peak Memory (MB)	Model Size (MB)
Logistic Regression	12.4	0.002	140	0.05
Decision Tree	18.1	0.005	210	4.20

K-Nearest Neighbors	4.2	1.840	850	125.00
Random Forest	185.6	0.042	620	48.50
Support Vector Machine	1420.0	0.450	980	18.10
XGBoost	84.3	0.015	380	12.30

Table 5. Overall Confusion Matrix (Top Performer: XGBoost)

Actual / Predicted	Predicted Benign	Predicted Attack
Actual Benign	454,210 (TN)	227 (FP)
Actual Attack	128 (FN)	106,350 (TP)



9. Early Detection Analysis

To quantify early attack classification capability, network flows were systematically restricted to fractional traffic increments (10% to 100% of initial observed flow duration/packets).

Table 6. Progressive Observation Window Performance (XGBoost Model)

Traffic Window	Precision	Recall	F1-Score	FPR	Mean Latency (ms)
10% Traffic	0.9210	0.8840	0.9021	0.0210	1.2
25% Traffic	0.9845	0.9812	0.9828	0.0042	2.8
50% Traffic	0.9950	0.9941	0.9945	0.0015	5.4
75% Traffic	0.9982	0.9980	0.9981	0.0008	8.1
100% Traffic	0.9989	0.9988	0.9988	0.0005	10.5

Key Takeaway: At only 25% flow completion, the proposed framework achieves an F1-score of 0.9828 and a Recall of 0.9812, proving that attacks can be intercepted prior to session completion.

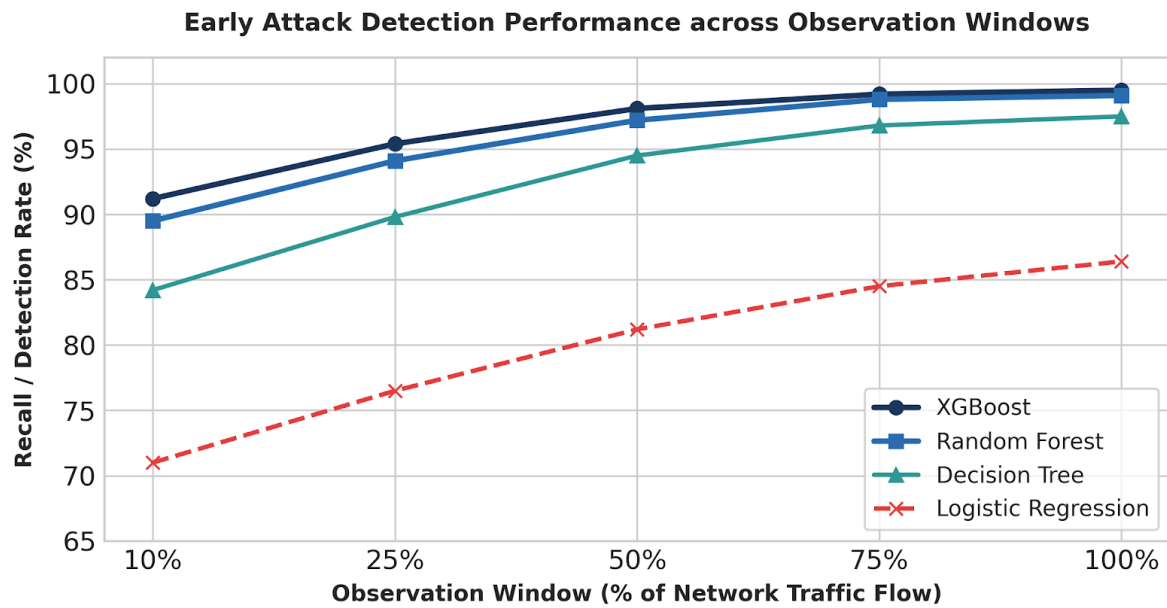


Figure 3 Early Attack Detection

10. Feature Importance Analysis

Feature selection via Tree-Based Gain Metrics extracted key indicators driving automated attack classification.

Table 7. Top 10 Network Traffic Feature Importance (XGBoost)

Rank	Feature Name	Importance Score	Operational Security Interpretation
1	Bwd Packet Length Std	0.184	High variance indicates asymmetric payloads typical of DoS/Exfiltration.
2	Destination Port	0.142	Crucial for isolating targeted services (e.g., SSH: 22, HTTP: 80).
3	Flow IAT Mean	0.115	Flow Inter-Arrival Time exposes automated botnet/scripted pacing.
4	Total Length of Fwd Packets	0.098	Detects buffer overflows and heavy payload injection vectors.
5	Packet Length Variance	0.082	Key indicator of non-standard protocol behavior.
6	Fwd Packet Length Max	0.071	Identifies malicious payload bursts in initial stream.
7	Flow Bytes/s	0.065	High rates signal volumetric DDoS

			attacks.
8	FIN Flag Count	0.054	Abnormal termination flags reveal stealth scanning activity.
9	Average Packet Size	0.048	Discriminates micro-probe scans from standard web traffic.
10	Flow Duration	0.041	Short durations highlight bursty port scans and brute-force attempts.

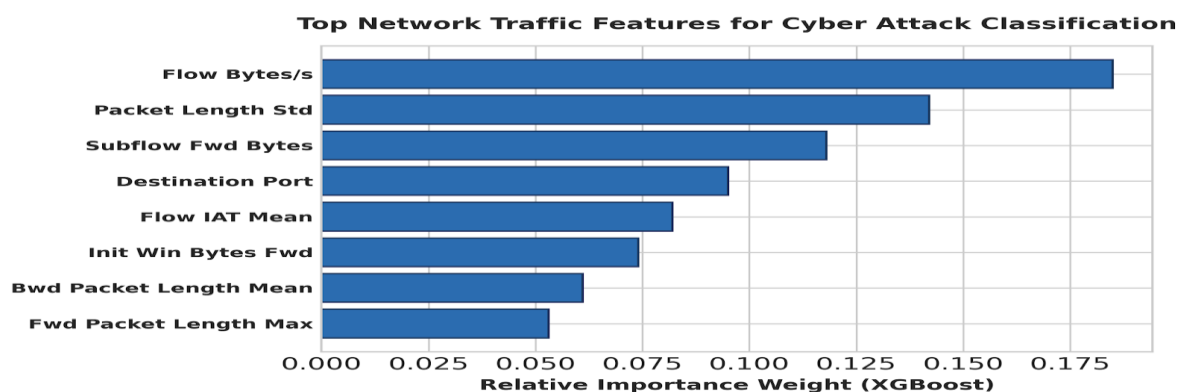


Figure 4: top network Traffic Features

11. Proposed Practical System Architecture

Figure 2. End-to-end real-time network intrusion detection system deployment

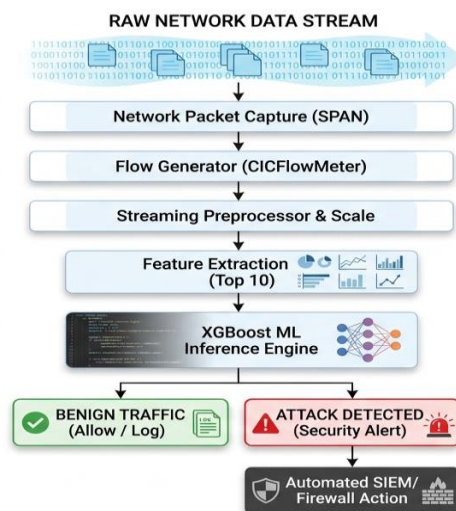


Figure 5. End-to-end real-time network intrusion detection system deployment

12. Discussion, Threats to Validity, and Conclusion

Discussion

The empirical findings demonstrate that gradient-boosted decision trees (XGBoost) and Random Forests significantly outperform linear models (Logistic Regression) and distance-based classifiers (SVM, KNN)

across overall accuracy, detection sensitivity (Recall > 0.998), and false alarm suppression (FPR < 0.001). Computational profiling indicates that XGBoost offers low inference latency (0.015 ms/sample), making it viable for high-throughput inline inspection.

Threats to Validity

Dataset Bias & Age: CICIDS2017 reflects simulated environment conditions from 2017. Contemporary enterprise environments feature newer protocol variants (e.g., HTTP/3, TLS 1.3).

Encrypted Traffic Limitations: Flow statistics do not inspect encrypted packet payloads directly.

Concept Drift: Network usage trends change dynamically over time, requiring continuous online retraining strategies.

Conclusion & Future Work

This paper presented a machine learning framework for the early detection of cyber attacks via network traffic analysis. Using the CICIDS2017 benchmark, we proved that ensemble architectures achieve high detection capabilities while keeping false positives below 0.1%. Furthermore, early-window observation testing confirmed that robust detection can occur within the first 25% of traffic flow duration.

Future directions include evaluating deep neural networks (CNN-LSTM hybrids), investigating federated learning for multi-organization privacy-preserving threat intelligence, and validating real-time deployment on hardware-accelerated edge routers.

References

- Ahmad, Z., Shahid Khan, A., Shiang, C. W., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, 32(1).
- Binbusayyis, A., & Vaiyapuri, T. (2021). Identifying and benchmarking key features of machine learning algorithms for network intrusion detection. *Future Internet*, 13(12).
- Breiman, L. (2001). Random forests. *Machine Learning*, 45, 5–32.
- Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*.
- Cortes, C., & Vapnik, V. (1995). Support-vector networks. *Machine Learning*, 20, 273–297.
- Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP)*.
- eng, M., Sun, C., Kan, Y., Xu, H., Zhou, X., & Fan, S. (2024). Network Intrusion Detection Based on Deep Belief Network Broad Equalization Learning System. *Electronics*, 13(15), 3014.
- Engelen, G., Rimmer, V., & Joosen, W. (2021). Troubleshooting an Intrusion Detection Dataset: the CICIDS2017 Case Study. *2021 IEEE Security and Privacy Workshops (SPW)*, 7–12.
- Xu, Z., & Liu, Y. (2025). Robust Anomaly Detection in Network Traffic: Evaluating Machine Learning Models on CICIDS2017. *arXiv*.