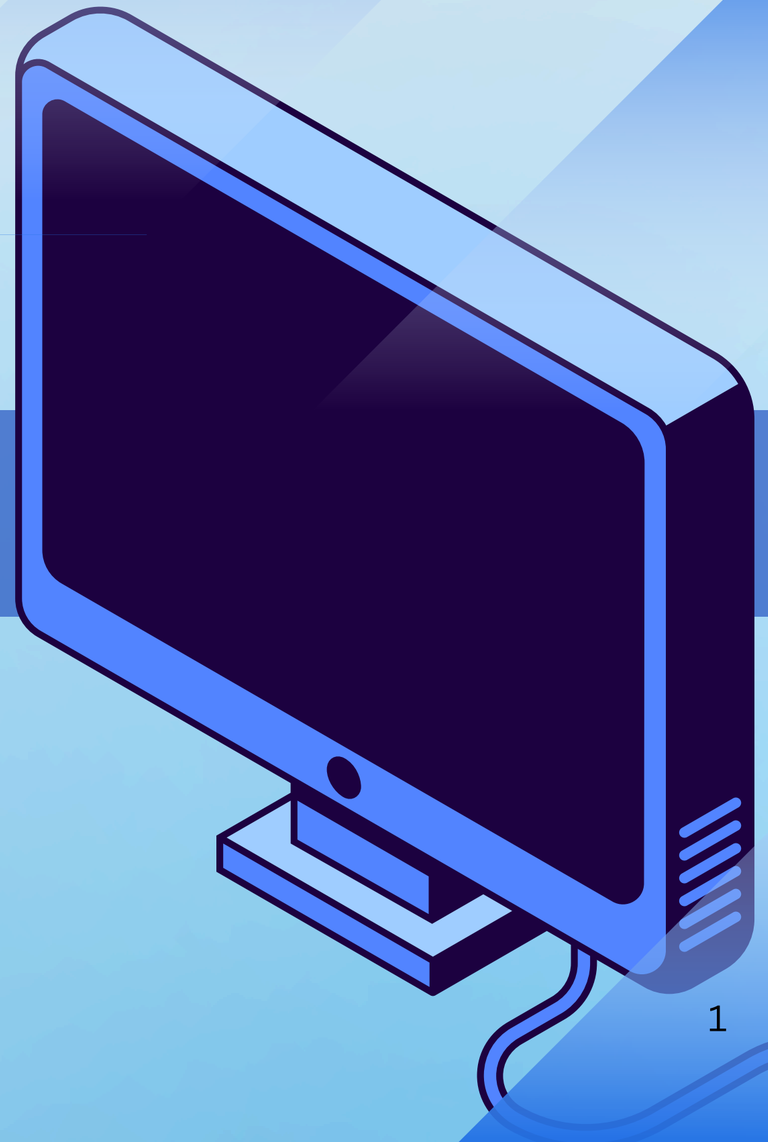
College of Engineering
Effat University

جامعة عفت
EFFAT UNIVERSITY

Machine Learning-Based Intrusion Detection



Amani Albarazi, Haifa Muhammad, Raghad Alamoudi, Maram Alhusami

Supervised by: Dr. Naila Marir

Course: CS4082 - Machine Learning

6th May, 2025

Table of Content

Introduction

Introduction

Growing Cyber Threats: Cyberattacks like malware, DoS, and phishing are becoming more sophisticated, posing risks to network integrity and security.

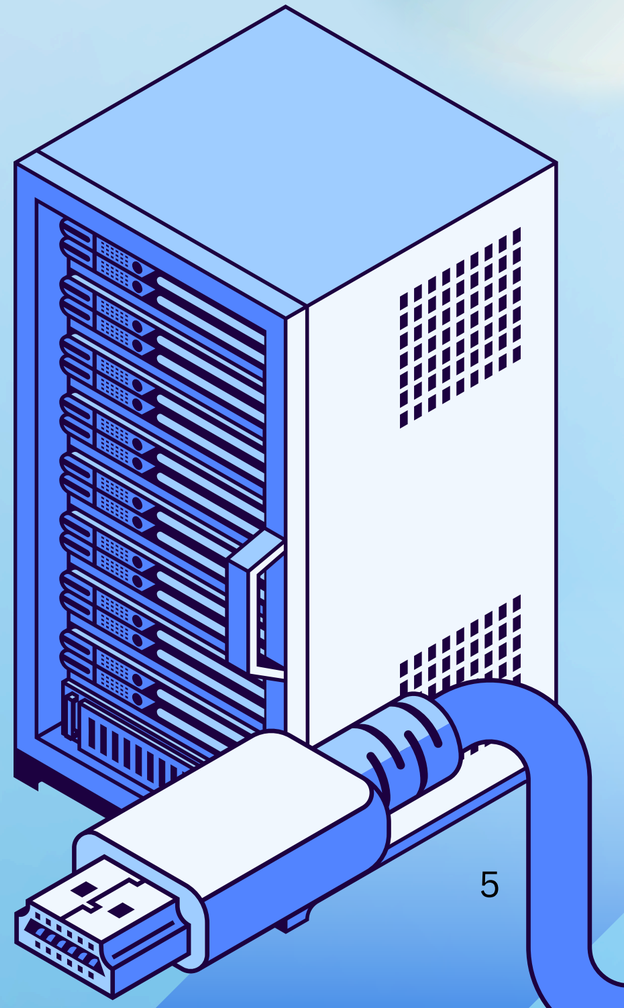
Limitations of Traditional IDS: Signature-based intrusion detection systems (IDS) struggle to detect zero-day attacks and evolving threats.

Promise of Machine Learning: ML offers dynamic solutions by learning patterns from network traffic, enabling proactive threat detection.

Problem Definition

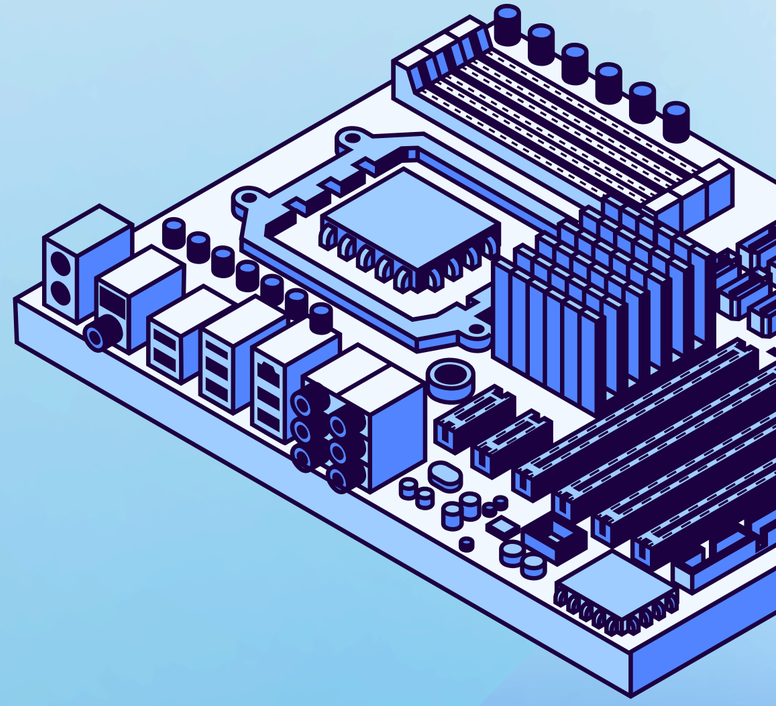
In cybersecurity, one of the most critical tasks is detecting malicious activities within network traffic to prevent breaches and ensure system integrity.

Main Issue: The Attack Classification Problem (ACP): The challenge of accurately distinguishing between normal network traffic and various types of attacks (e.g., DDoS, malware, spoofing) in real-time, while minimizing false alarms and missed threats.



Limitations of Current Solutions

- **Signature-Based IDS:** Fail against zero-day attacks and polymorphic malware.
- **Supervised ML Models:** Require large labeled datasets and struggle with unseen attack types.
- **Unsupervised Methods:** Limited accuracy in distinguishing attacks from benign anomalies.
- **Real-World Gaps:** Most solutions are tested in controlled environments, lacking real-time scalability and adaptability.



Our Goals

Comprehensive Evaluation: Compare traditional ML (Random Forest, XGBoost), deep learning (CNN, MLP), and unsupervised models (Isolation Forest) on diverse attack datasets.

Balance Metrics: Optimize precision (reduce false alarms) and recall (minimize missed attacks).

Real-World Readiness: Address class imbalance, feature engineering, and model interpretability.

Significance

SDG 9 (Industry, Innovation, Infrastructure): Supports resilient infrastructure by safeguarding networks from disruptions (e.g., DDoS attacks).

SDG 16 (Peace, Justice, Strong Institutions): Promotes secure digital ecosystems, critical for trust in institutions and data privacy.

Aligns with national goals to enhance cybersecurity frameworks, protecting critical sectors (healthcare, finance, smart cities).

Literature Review

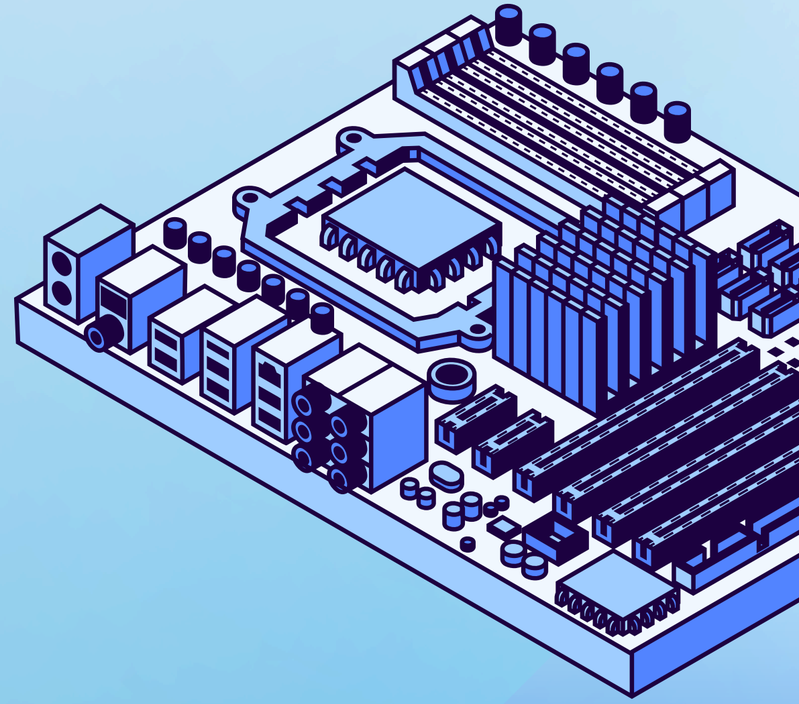
Comparison of Machine Learning and Deep Learning Algorithms for Intrusion Detection Systems

Methods Compared	Dataset Used	Best Accuracy	Key Findings	Gaps	Refs
Naive Bayes, Logistic Regression, kNN, RF, XGBoost, CNN, ANN, LSTM, GRU, LightGBM	CICIoT2023	**RF: 99.29%** **XGBoost**: 99.26%	RF and XGBoost performed best for IoT attack detection. Deep learning models like CNN performed well but struggled with precision	Limited to one dataset (CICIoT2023). Lack of real-time evaluation and generalization across different attack types.	[7]
KNN, XGBoost, CART, CNN, LSTM	CIDDS, CICIDS2017	**CART: 99.31%** **CNN and LSTM:** 99%	CART showed highest accuracy with lowest training time. CNN and LSTM performed well but took longer to train	Focused mainly on accuracy and precision; lacks evaluation on real-time performance, scalability, and broader attack scenarios.	[8]
Logistic Regression, Decision Trees, RF, XGBoost, CNN, MLP	Benchmark datasets (unspecified)	**RF (highest, not specified), Logistic Regression and Decision Trees:** >90%	RF outperformed other traditional ML models in accuracy. Deep learning models like CNN were better but took longer to implement.	Limited to benchmark datasets. Does not cover all possible deep learning methods. Lacks real-time applicability assessment.	[9]
Decision Tree, K-NN, RF, Naïve Bayes, LSTM, GRU	WSN-DS, KDD Cup Network Intrusion Dataset	**RF** (highest ML accuracy) **LSTM** (highest DL -accuracy)	RF outperformed traditional ML models; LSTM achieved best performance among deep learning models for intrusion detection	Limited to traditional datasets. Does not include extensive comparison across a wide range of deep learning techniques.	[10]

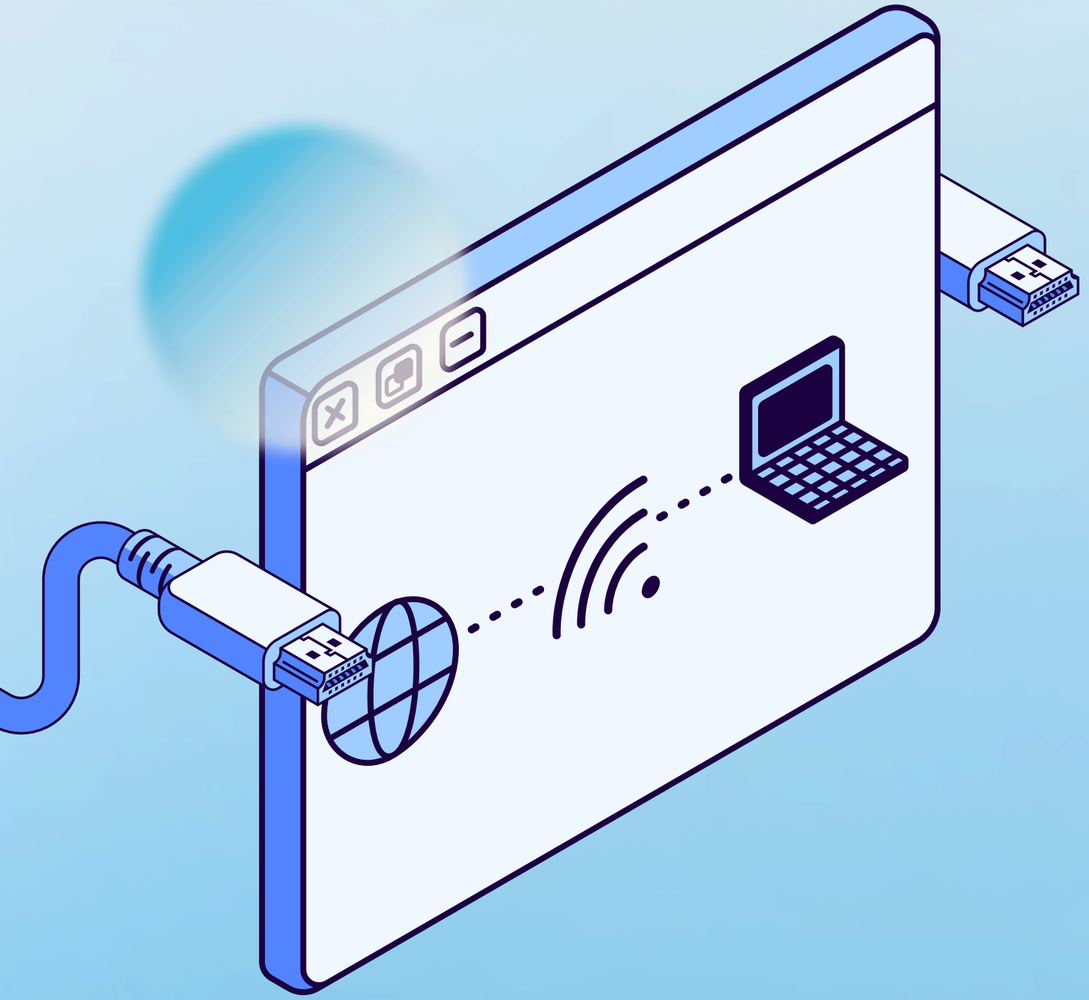
Methodology

Our Datasets

- Backdoor Malware - around 178,898 records
- DoS-TCP Flood - about 222,215 records
- DoS-UDP Flood - approximately 188,474 records
- DDoS-TCP Flood - around 106,374 records



Preprocessing the Data



- Cleaned each dataset separately by dropping null columns.
- Created a new column in each dataset named “Attack Type”.
- Merged the 4 datasets using “concat”

Traditional Machine Learning Algorithms

Rely on manual feature engineering, where domain knowledge is used to extract relevant input features from raw data. These models are generally more interpretable, require less data, and perform well on structured or tabular data. Models used:

Logistic Regression

Decision Trees

Support Vector Machines (SVM)

K -Nearest Neighbors (KNN)

Random Forests

Gradient Boosting (GB)

AdaBoost

LightGBM

Advanced Supervised Models

These models are designed to handle complex data patterns, improve prediction performance, and address limitations such as overfitting and computational inefficiency seen in simpler models.

Models used:

ExtraTrees Classifier

Ridge Classifier

Linear Discriminant Analysis (LDA)

Quadratic Discriminant Analysis (QDA)

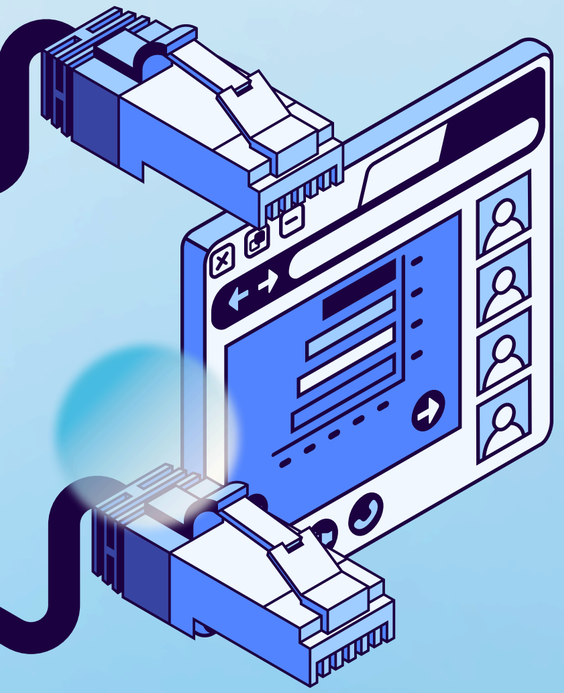
Neural Network-Based Methods

Refer to machine learning techniques that use artificial neural networks (ANNs) to model and learn complex patterns in data. These methods are part of deep learning, a subfield of machine learning.

Models used:

MLPClassifier

Sequential



input Data

Network traffic data

Preprocessing

- Data cleaning,
- feature extraction
- Class imbalance handling
- Standrazation.

Model Training

- Supervised Models (e.g. Random Forest, SVM, Logistic Regression)
- Neural Models (MLPClassifier, Sequential)

Model Evaluation

- Confusion Matrix
- Calculate Precision
- Recall
- F1-Score

Output

Attack/Non-Attack.

Results

Performance Comparison of Different Models

Model	Accuracy (%)	Precision	Recall	F1-Score
Logistic Regression (LR)	85.2	0.84	0.85	0.84
K-Nearest Neighbors (KNN)	82.7	0.81	0.83	0.82
Decision Tree (DT)	86.5	0.85	0.86	0.85
Random Forest (RF)	91.4	0.91	0.91	0.91
Gradient Boosting (GB)	89.9	0.89	0.90	0.89
AdaBoost	88.3	0.87	0.88	0.87
LightGBM	90.2	0.90	0.90	0.90
ExtraTrees Classifier	90.8	0.90	0.91	0.90
Scikit-learn MLP Classifier	89.7	0.89	0.90	0.89
Neural Network Classification (Tensor Flow/Keras)	92.5	0.92	0.93	0.92

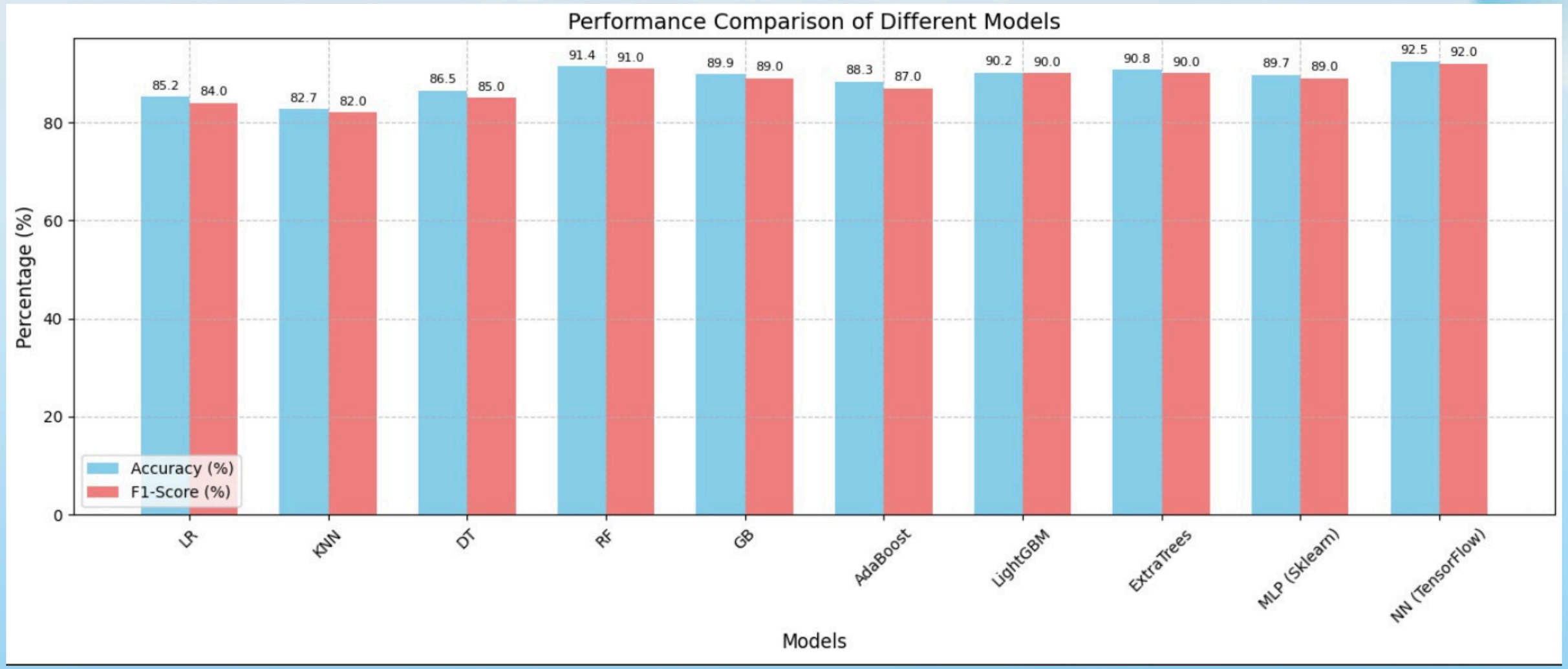


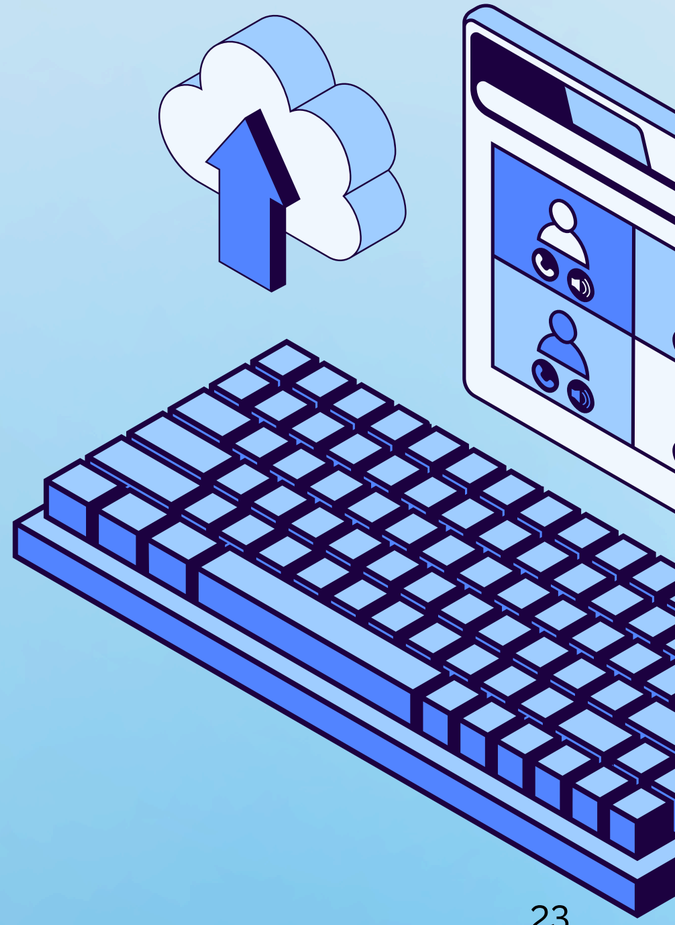
Figure 1: Performance Comparison of Different Models based on Accuracy and F1-Score

LLMs Output Analysis for Network Traffic Classification

Example	LLM output	Attack/ Not attack	Attack type	Explanation
1	Suspicious: High UDP traffic with abnormal packet size variance. Potential backdoor communication.	Attack	Backdoor Malware	The high use of UDP, small packet sizes, and abnormal variance indicate stealthy data exfiltration attempts typical of backdoors.
2	Abnormal traffic pattern detected: Rapid TCP packet bursts with no handshake. Possible Dos attack.	Attack	DoS – TCP Flood	Continuous TCP packets without completing the handshake suggest flooding, trying to exhaust server resources.
3	Mostly benign behavior detected. Moderate traffic rate, consistent protocol usage, no flag anomalies."	Not Attack	-	The traffic is stable, with no spikes or abnormal flags, typical of regular network usage.
4	Extreme packet rate and small inter-arrival time between packets. Likely a DDoS TCP Flood attack.	Attack	DoS – TCP Flood	Very high request rate and synchronized packet timing match typical DDoS behavior across distributed sources.
5	Slight anomaly detected: High DNS request rate, but no strong indicators of malicious activity.	Not Attack	-	Some irregular behavior seen in DNS requests, but not enough for clear attack classification - needs monitoring.

Conclusion

- Traditional machine learning and neural network models achieved strong performance in detecting attacks.
- Supervised models achieved higher accuracy, precision, recall, and F1-scores, benefiting from labeled data to learn attack patterns directly.
- Neural networks captured complex traffic patterns better but required more resources.
- Machine learning methods proved effective for detecting various attacks in realistic network conditions.



References

[1] J. P. Ntayagabiri, Y. Bentaleb, J. Ndikumagenge, and H. El Makhtoum, "A Comparative Analysis of Supervised Machine Learning Algorithms for IoT Attack Detection and Classification," Journal of Computer and Theoretical Applications (JCTA), vol. 2, no. 3, pp. 396–407, Feb. 2025, doi: 10.62411/jcta.11901.

[2] N. Thapa, Z. Liu, D. B. KC, B. Gokaraju, and K. Roy, "Comparison of Machine Learning and Deep Learning Models for Network Intrusion Detection Systems," Future Internet, vol. 12, no. 10, p. 167, Sep. 2020, doi: 10.3390/fi12100167.

[3] J. Note and M. Ali, "Comparative Analysis of Intrusion Detection System Using Machine Learning and Deep Learning Algorithms," Annals of Emerging Technologies in Computing (AETiC), vol. 6, no. 3, pp. 19–36, Jul. 2022, doi: 10.33166/AETiC.2022.03.003.

[4] B. Mahbooba, R. Sahal, W. Alosaimi, and M. Serrano, "Trust in Intrusion Detection Systems: An Investigation of Performance Analysis for Machine Learning and Deep Learning Models," Complexity, vol. 2021, Article ID 5538896, 23 pages, 2021, doi: 10.1155/2021/5538896.

Thank You!