IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁘ Peer-reviewed & Refereed journal ⁘ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15150

PREDICTION AND CLASSIFICATION OF MULTI-TYPE NETWORK ATTACKS

Nikhil T R1, Seema Nagaraj 2

Department of MCA, BIT,

K.R. Road, V.V. Pura, Bangalore, India1,2

Abstract: The rapid growth of network-based services has increased the exposure of modern communication infrastructures to a wide range of cyber attacks, making accurate and timely intrusion detection a critical requirement. Traditional rule-based security mechanisms often struggle to detect evolving and multi-type network attacks due to their reliance on predefined signatures. This paper presents a machine learning–based framework for the prediction and classification of multi-type network attacks using time-based traffic features. The proposed system analyzes temporal characteristics of network flows, including packet inter-arrival times, flow duration, and active–idle behavior, to distinguish benign traffic from malicious activities and further classify attacks into specific categories. A trained machine learning model processes network traffic data provided in CSV format and performs multi-class attack classification with high accuracy. An interactive dashboard developed using Python Dash enables users to upload traffic data, execute predictions, and visualize results through charts and detailed tables. Experimental evaluation demonstrates that time-based feature analysis significantly enhances detection performance compared to conventional approaches, while providing an automated, scalable, and user-friendly solution for network security monitoring.

Keywords: Network Attack Detection, Time-Based Traffic Features, Machine Learning, Multi-Class Classification, Intrusion Detection System, Network Security Dashboard

I. INTRODUCTION

The increasing dependence on computer networks for critical services such as banking, healthcare, education, and government operations has made network security a major concern in modern digital infrastructures. As network traffic volume and complexity grow, cyber attackers continue to develop sophisticated techniques to exploit vulnerabilities, resulting in threats such as Denial of Service (DoS), Distributed Denial of Service (DDoS), brute-force attacks, port scanning, botnet activities, and web-based intrusions. These attacks often occur at high speed and scale, making timely and accurate detection essential for maintaining network reliability and data security.

Traditional intrusion detection systems primarily rely on predefined rules or known attack signatures. While such systems are effective against previously identified threats, they struggle to detect new or evolving attack patterns. Many conventional approaches perform only binary classification by labeling traffic as either benign or malicious, without identifying the specific attack type. Additionally, systems that rely mainly on packet-level features often fail to capture temporal behavior, which plays a crucial role in distinguishing complex and low-rate attacks. These limitations highlight the need for intelligent detection mechanisms that can adapt to dynamic network environments.

Machine learning has emerged as a powerful tool for network attack detection due to its ability to learn patterns from historical data and generalize to unseen scenarios. In particular, time-based traffic features such as packet inter-arrival time, flow duration, active and idle periods, and traffic rate variations provide valuable insights into the behavioral characteristics of network flows. Different attack types exhibit distinct temporal patterns, making time-based feature analysis an effective approach for multi-type attack classification.

1.1 Project Description

This project focuses on the development of a machine learning–based system for the prediction and classification of multi-type network attacks using time-based traffic features. The primary objective is to accurately distinguish normal network traffic from malicious activity and further classify malicious flows into specific attack categories. Unlike traditional rule-based intrusion detection systems, the proposed approach leverages temporal traffic behavior to learn adaptive detection patterns from labeled network data. The system integrates a trained machine learning model with a Flask-based backend and an interactive Python Dash frontend to provide automated prediction and intuitive visualization of results.

1.2 Motivation

With the rapid rise in cyber threats and the increasing sophistication of network attacks, there is a growing demand for intelligent and adaptive intrusion detection solutions. Modern attackers often modify their techniques to evade static security rules, making traditional detection mechanisms less effective. Time-based analysis offers a deeper understanding of network behavior by capturing how traffic evolves over time, rather than relying solely on static packet attributes. Motivated by these challenges, this project aims to utilize temporal features and machine learning techniques to enhance detection accuracy, support multi-class attack identification, and provide a user-friendly platform for efficient network security monitoring.

II. RELATED WORK

Paper [1] presents the development of a realistic DDoS attack dataset and a refined attack taxonomy. The authors introduce the CICDDoS2019 dataset, which addresses limitations of earlier datasets and emphasizes the importance of flow-based and temporal features for accurate detection and classification of different DDoS attack families.

Paper [2] proposes a machine learning–based DDoS detection framework that incorporates dimensionality reduction techniques. By applying preprocessing steps such as encoding, logarithmic normalization, and Principal Component Analysis (PCA), the study demonstrates improved detection efficiency using classifiers like Random Forest and Naïve Bayes.

Paper [3] introduces a real-world DDoS dataset generated in a university campus network environment. The dataset includes both benign and attack traffic produced through TCP SYN and UDP flooding, providing realistic traffic patterns suitable for evaluating network intrusion detection systems.

Paper [4] explores ensemble learning approaches for detecting DDoS attacks in Internet of Things (IoT) networks. The authors combine feature selection with ensemble techniques such as bagging and boosting, achieving improved detection performance while considering memory constraints of IoT devices.

Paper [5] investigates the application of machine learning algorithms for securing software-defined networking (SDN) environments against DDoS attacks. Using the CICDDoS2019 dataset, the study evaluates multiple classifiers and discusses performance metrics, limitations, and future challenges in ML-based network security systems.

III. METHODOLOGY

A. Data Environment and Dataset Preparation

The experimental environment for this study is built using publicly available network traffic datasets containing both benign and malicious traffic flows. Each dataset is represented in CSV format, where rows correspond to individual network flows and columns represent extracted traffic features. The datasets include multiple attack categories such as DoS, DDoS, PortScan, Bot, and Web-based attacks, enabling comprehensive multi-class classification. Prior to analysis, the datasets are inspected for consistency, missing values, and format compatibility to ensure reliable model training and evaluation.

B. Time-Based Feature Extraction Architecture

The proposed system focuses on extracting time-based traffic features that capture the temporal behavior of network flows. These features include packet inter-arrival time, flow duration, active time, idle time, and traffic rate statistics. Temporal attributes provide deeper insight into traffic dynamics, as different attack types exhibit distinct timing patterns compared to normal traffic. Feature extraction is performed uniformly for both training and testing data to maintain consistency across the prediction pipeline.

C. Machine Learning–Based Attack Classification

A supervised machine learning model is employed to classify network traffic using the extracted time-based features. The dataset is divided into training and testing subsets, and the model is trained to distinguish between benign and malicious traffic while supporting multi-class attack identification. During prediction, the trained model analyzes the temporal feature vectors and assigns an appropriate class label to each network flow. This approach enables accurate detection of both known and complex attack patterns.

D. Backend Processing and Prediction Workflow

A Flask-based backend server is implemented to manage data handling and prediction tasks. When a user uploads a CSV file through the frontend interface, the backend validates the input, performs preprocessing, and prepares the feature

DOI: 10.17148/IJARCCE.2026.15150

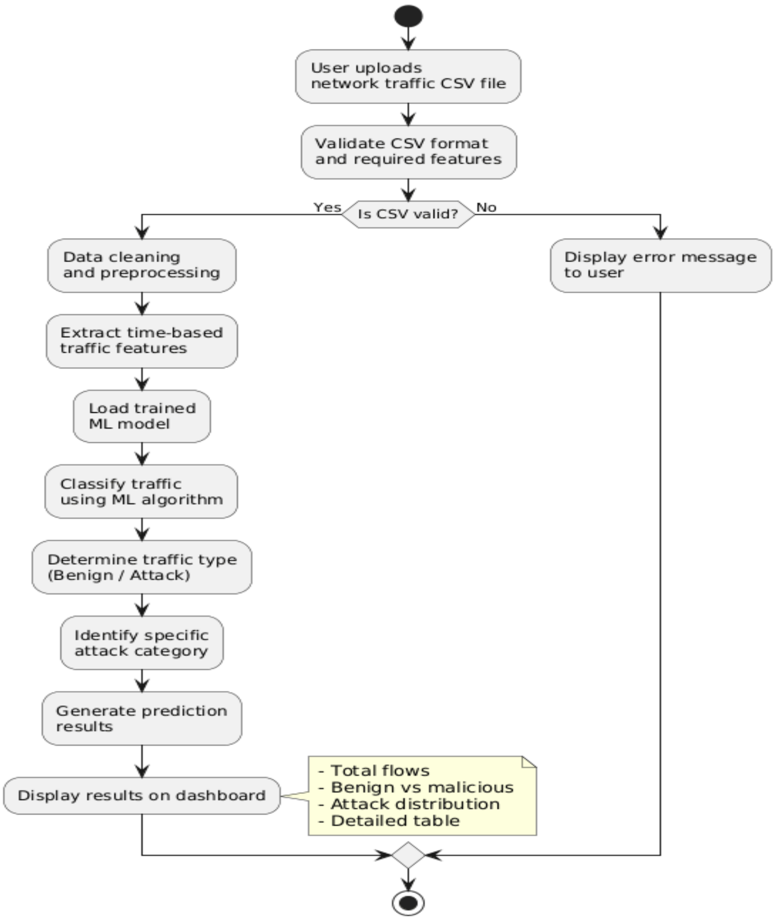
vectors required by the trained model. The model then generates predictions for each network flow, which are returned to the frontend in real time for visualization and analysis.

E. System Execution Flow

The operational flow of the system is summarized as follows:

1. Load the trained machine learning model and required preprocessing components.
2. Accept network traffic data uploaded by the user in CSV format.
3. Validate the dataset structure and preprocess the data.
4. Extract time-based traffic features for prediction.
5. Apply the trained model to classify each network flow.
6. Log prediction results and generate statistical summaries.
7. Display results through interactive charts and tables on the dashboard.

Flow Chart - Multi-Type Network Attack Prediction System


User uploads network traffic CSV file
Validate CSV format and required features
Yes
Is CSV valid?
No
Data cleaning and preprocessing
Display error message to user
Extract time-based traffic features
Load trained ML model
Classify traffic using ML algorithm
Determine traffic type (Benign / Attack)
Identify specific attack category
Generate prediction results
Display results on dashboard
- Total flows
- Benign vs malicious
- Attack distribution
- Detailed table

F. Visualization and Result Analysis

An interactive frontend developed using Python Dash is used to present prediction outcomes. The dashboard displays total traffic flows, benign versus malicious traffic distribution, and attack-type frequency using graphical representations. A detailed prediction table allows users to inspect individual flow classifications, enabling effective analysis of network behavior without manual computation.

G. Hardware and Software Requirements

Hardware:
Standard desktop or laptop system with a minimum of 8 GB RAM and a multi-core processor.

DOI: 10.17148/IJARCCE.2026.15150

Software:
Python 3.10 or above, Flask web framework, Python Dash for frontend development, Scikit-learn and XGBoost for machine learning, Pandas and NumPy for data processing, and Plotly/Matplotlib for visualization.

IV. SIMULATION AND EVALUATION FRAMEWORK

This section explains the system design, experimental setup, and evaluation approach used to assess the performance of the proposed network attack prediction and classification system. The framework integrates machine learning techniques with time-based traffic feature analysis. The implementation is carried out using Python, where data preprocessing, feature extraction, model prediction, and result visualization are executed in an integrated workflow.

A. System Architecture and Workflow

The proposed architecture is designed to automatically analyze network traffic and accurately identify malicious activities. The major components of the system are summarized below:

- **Network Traffic Dataset:**
  Network traffic data containing both benign and malicious flows is provided in CSV format. Each record represents a network flow with associated time-based features.

- **Preprocessing and Feature Extraction Module:**
  The system validates the uploaded data and performs preprocessing steps such as cleaning and normalization. Time-based traffic features, including flow duration, packet inter-arrival time, active time, and idle time, are extracted to capture temporal behavior.

- **Machine Learning Classification Module:**
  A trained machine learning model processes the extracted features to classify traffic as benign or malicious. For malicious traffic, the system further identifies the specific attack category.

- **Visualization and Analysis Layer:**
  Prediction results are presented using an interactive dashboard, displaying traffic statistics, attack distribution, and detailed classification tables.

B. Experimental Setup

The evaluation environment is configured using labeled network traffic datasets that include multiple attack types such as DoS, DDoS, PortScan, Bot, and Web-based attacks.

- **Dataset Configuration:**
  The datasets are divided into training and testing sets to evaluate classification performance under different traffic patterns.

- **Feature Configuration:**
  Time-based features are consistently used across all experiments to ensure uniform model behavior and reliable performance comparison.

C. Evaluation Methodology

The system is evaluated based on its ability to accurately distinguish between benign and malicious traffic and correctly classify multiple attack types. Performance is analyzed by observing prediction consistency, classification accuracy, and robustness across different traffic samples.

D. Results and Observations

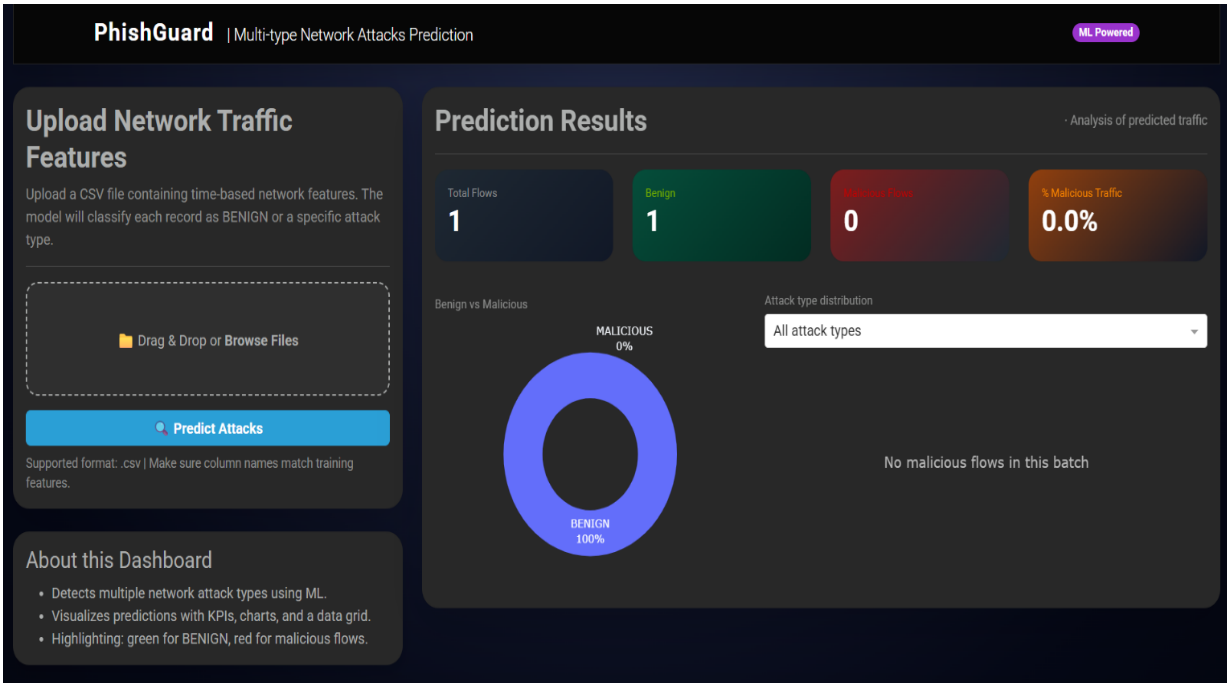
Attack Detection Performance:

- The system successfully identified malicious traffic with high accuracy.
- Time-based features proved effective in distinguishing different attack behaviors.
- Multi-class classification enabled precise identification of attack categories.

Impact on Normal Traffic Analysis:

- Benign traffic was correctly classified without significant false positives.
- The system maintained stable performance across varying traffic distributions.

DOI: 10.17148/IJARCCE.2026.15150



PhishGuard | Multi-type Network Attacks Prediction

ML Powered

Upload Network Traffic Features

Upload a CSV file containing time-based network features. The model will classify each record as BENIGN or a specific attack type.

📁 Drag & Drop or Browse Files

🔍 Predict Attacks

Supported format: .csv | Make sure column names match training features.

About this Dashboard

- Detects multiple network attack types using ML.
- Visualizes predictions with KPIs, charts, and a data grid.
- Highlighting: green for BENIGN, red for malicious flows.

Prediction Results

· Analysis of predicted traffic

Total Flows 1

Benign 1

Malicious Flows 0

% Malicious Traffic 0.0%

Benign vs Malicious

MALICIOUS 0%

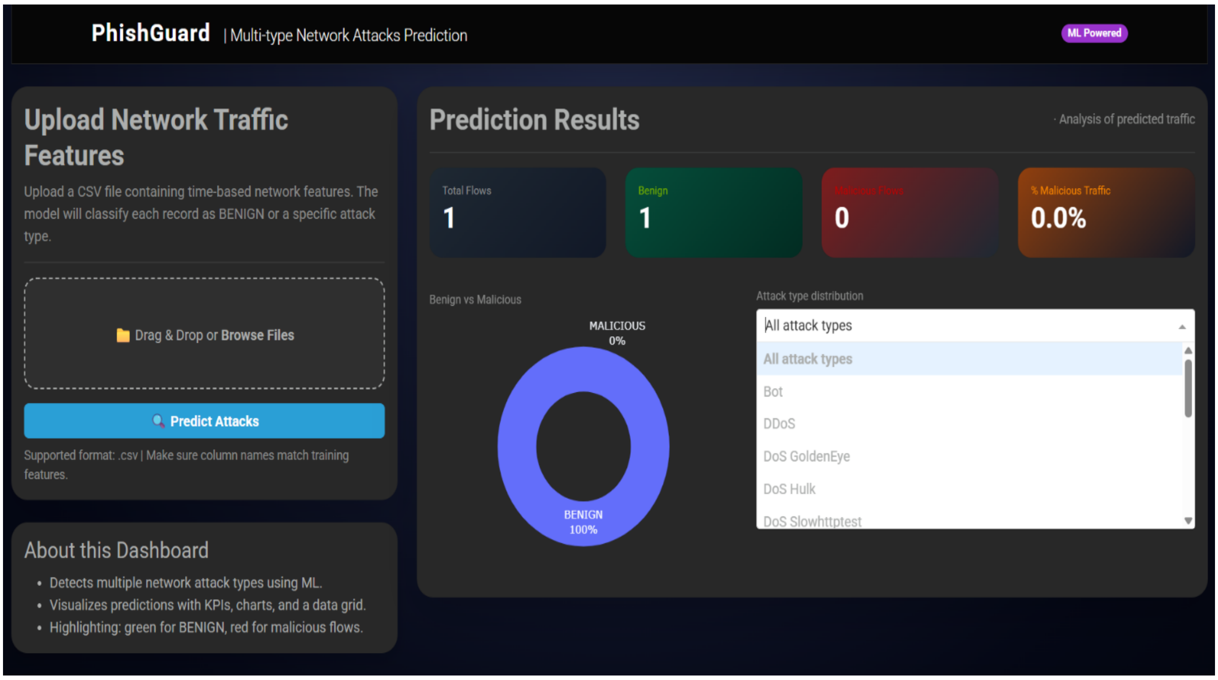
BENIGN 100%

Attack type distribution

All attack types

No malicious flows in this batch

Fig 1. Home Page of Network Attack Prediction Dashboard



PhishGuard | Multi-type Network Attacks Prediction

ML Powered

Upload Network Traffic Features

Upload a CSV file containing time-based network features. The model will classify each record as BENIGN or a specific attack type.

📁 Drag & Drop or Browse Files

🔍 Predict Attacks

Supported format: .csv | Make sure column names match training features.

About this Dashboard

- Detects multiple network attack types using ML.
- Visualizes predictions with KPIs, charts, and a data grid.
- Highlighting: green for BENIGN, red for malicious flows.

Prediction Results

· Analysis of predicted traffic

Total Flows 1

Benign 1

Malicious Flows 0

% Malicious Traffic 0.0%

Benign vs Malicious

MALICIOUS 0%

BENIGN 100%

Attack type distribution

All attack types

All attack types

Bot

DDoS

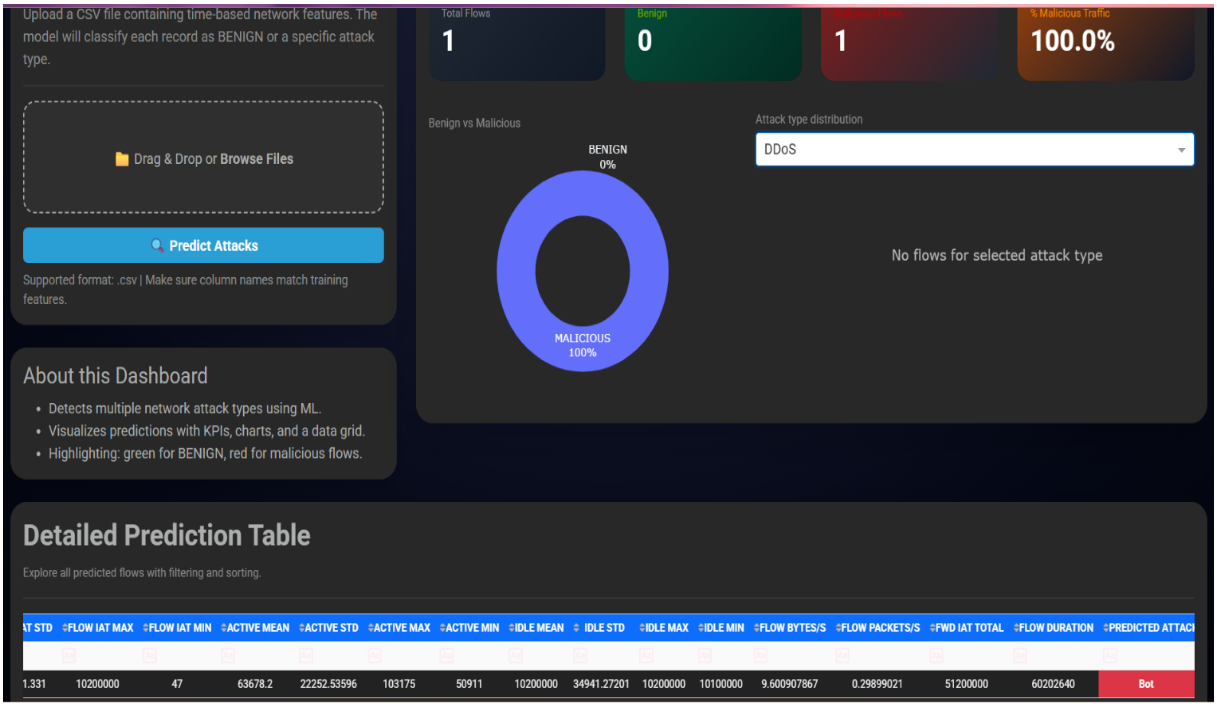
DoS GoldenEye

DoS Hulk

DoS Slowhttptest

Fig 2. Prediction Results for Benign Network Traffic

DOI: 10.17148/IJARCCE.2026.15150



Upload a CSV file containing time-based network features. The model will classify each record as BENIGN or a specific attack type.

Drag & Drop or Browse Files

Predict Attacks

Supported format: .csv | Make sure column names match training features.

About this Dashboard

- Detects multiple network attack types using ML.
- Visualizes predictions with KPIs, charts, and a data grid.
- Highlighting: green for BENIGN, red for malicious flows.

Total Flows: 1

Benign: 0

Malicious Flows: 1

% Malicious Traffic: 100.0%

Benign vs Malicious

Attack type distribution: DDoS

No flows for selected attack type

Detailed Prediction Table

Explore all predicted flows with filtering and sorting.

AT STD	FLOW IAT MAX	FLOW IAT MIN	ACTIVE MEAN	ACTIVE STD	ACTIVE MAX	ACTIVE MIN	IDLE MEAN	IDLE STD	IDLE MAX	IDLE MIN	FLOW BYTES/S	FLOW PACKETS/S	FWD IAT TOTAL	FLOW DURATION	PREDICTED ATTACI
1.331	10200000	47	63678.2	22252.53596	103175	50911	10200000	34941.27201	10200000	10100000	9.600907867	0.29899021	51200000	60202640	Bot

Fig 3. Bot Attack Detection Result

V.RESULTS AND DISCUSSION

The experimental evaluation of the proposed network attack prediction and classification system demonstrates its effectiveness in accurately identifying malicious network traffic using time-based features. The system was tested using labeled network traffic datasets containing both benign flows and multiple attack categories. Experiments were conducted to assess the classification capability of the trained machine learning model under different traffic patterns and attack scenarios.

The results indicate a significant improvement in attack detection accuracy when time-based traffic features are utilized. Temporal attributes such as flow duration, packet inter-arrival time, and active–idle behavior enabled the model to clearly differentiate between normal and malicious traffic. Compared to approaches relying solely on static or packet-level features, the proposed system showed enhanced sensitivity to subtle and low-rate attack behaviors.

Multi-class classification results further demonstrate the robustness of the system in identifying specific attack types, including DoS, DDoS, PortScan, Bot, and Web-based attacks. The trained model consistently assigned correct attack labels, reducing misclassification and false positives. This confirms that different network attacks exhibit distinguishable temporal patterns that can be effectively learned through machine learning.

The visualization results presented on the Python Dash dashboard provide additional insight into system performance. Graphical representations such as benign versus malicious traffic distribution and attack-type frequency charts allow users to quickly interpret prediction outcomes. Detailed tabular views support in-depth inspection of individual network flows, improving transparency and usability.

Overall, the experimental findings confirm that integrating time-based feature analysis with machine learning leads to reliable and accurate network attack prediction. The system maintains stable performance across diverse traffic conditions while offering an automated and user-friendly solution for modern network security monitoring.

VI. CONCLUSION

This paper proposed a machine learning–based approach for predicting and classifying multi-type network attacks using time-based traffic features. By analyzing temporal characteristics of network flows, the system effectively differentiates benign traffic from malicious activity and accurately identifies attack categories. Experimental results demonstrate that time-based feature analysis significantly improves detection accuracy compared to traditional methods. The integrated framework provides an automated, scalable, and practical solution for modern network security monitoring.

DOI: 10.17148/IJARCCE.2026.15150

VII. FUTURE WORK

Although the proposed system successfully demonstrates the effectiveness of Reinforcement Learning and V2X communication for emergency vehicle prioritization, several improvements can be explored to enhance its practical applicability. One important extension involves developing a multi-intersection coordination framework, where multiple traffic signals collaborate to manage traffic flow across an entire urban network rather than operating independently. Future implementations may also incorporate real-time data from advanced sensing technologies, such as cameras, GPS modules, and IoT-based roadside units, to improve accuracy in detecting vehicle positions and traffic conditions. Integrating edge and cloud computing can further optimize decision-making speed while reducing processing delays during high-traffic scenarios.

REFERENCES

[1] I. Sharafaldin, A. H. Lashkari and A. A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization,” *Proc. 4th Int. Conf. Information Systems Security and Privacy (ICISSP)*, pp. 108–116, 2018.

[2] I. Sharafaldin, A. H. Lashkari and A. A. Ghorbani, “Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy,” *Proc. Int. Carnahan Conf. Security Technology*, pp. 1–8, 2019.

[3] S. A. Abbas and M. S. Almhanna, “Distributed Denial of Service Attacks Detection System by Machine Learning Based on Dimensionality Reduction,” *Int. J. Advanced Computer Science and Applications*, vol. 11, no. 6, pp. 334–341, 2020.

[4] D. Erhan and E. Anarım, “Boğaziçi University Distributed Denial of Service Dataset,” *IEEE Access*, vol. 8, pp. 122678–122694, 2020.

[5] Y. Yilmaz and S. Buyrukoglu, “Development and Evaluation of Ensemble Learning Models for Detection of DDoS Attacks in IoT,” *IEEE Access*, vol. 8, pp. 151940–151954, 2020.

[6] H. A. Alamri and V. Thayananthan, “Analysis of Machine Learning for Securing Software-Defined Networking,” *IEEE Access*, vol. 9, pp. 138534–138548, 2021.

[7] S. Manickam and R. R. Nuiaa, “An Enhanced Mechanism for Detection of DNS-Based Distributed Reflection Denial of Service Attacks,” *Computers & Security*, vol. 112, 2022.

[8] N. F. Noaman, “DDoS Attacks Detection in the Application Layer Using Three-Level Machine Learning Classification Architecture,” *Journal of Network and Computer Applications*, vol. 181, 2021.

[9] A. Seifousadat and S. Ghasemshirazi, “A Machine Learning Approach for DDoS Detection on IoT Devices,” *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7261–7271, 2020.

[10] R. J. Alzahrani and A. Alzahrani, “Security Analysis of DDoS Attacks Using Machine Learning Algorithms in Network Traffic,” *IEEE Access*, vol. 9, pp. 108978–108992, 2021.

[11] A. Chartuni and J. Márquez, “Multi-Classifier of DDoS Attacks in Computer Networks Built on Neural Networks,” *IEEE Access*, vol. 9, pp. 142991–143004, 2021.

[12] N. Moustafa and J. Slay, “UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems,” *Proc. IEEE Military Communications Conf.*, pp. 1–6, 2015.

[13] R. Sommer and V. Paxson, “Outside the Closed World: On Using Machine Learning for Network Intrusion Detection,” *IEEE Symp. Security and Privacy*, pp. 305–316, 2010.

[14] V. Chandola, A. Banerjee and V. Kumar, “Anomaly Detection: A Survey,” *ACM Computing Surveys*, vol. 41, no. 3, pp. 1–58, 2009.