International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

An Intelligent Machine Learning Framework for Detecting QUIC-Based Traffic Flood Attacks in Encrypted HTTP/3 Networks

Mr. M. V. Rajesh[1], Balla Aarathisree[2], S S V Sumanvitha Palivela [3], Nagala Bhavya Pragna[4], Kamalesh Chitra[5], Taneti Ritesh[6]

[1]Associate Professor, Department of CSE (Data Science) In Pragati Engineering College, Surampalem, Andhra Pradesh, India,

[2,3,4,5,6] UG Students Department of CSE (Data Science) In Pragati Engineering College, Surampalem, Andhra Pradesh, India.

ABSTRACT: The rapid growth of encrypted internet protocols such as HTTP/3 and QUIC has significantly improved communication speed and security on modern networks. However, these protocols also introduce new challenges for network security, particularly in detecting Distributed Denial of Service (DDoS) traffic flood attacks. Traditional monitoring techniques rely on packet inspection, which becomes difficult when network traffic is encrypted. This study proposes an intelligent machine learning framework for detecting QUIC-based traffic flood attacks in encrypted HTTP/3 network environments. The proposed system analyses network flow behaviour rather than packet content, enabling effective detection even when traffic payloads are encrypted. To build the detection model, network traffic data are captured and processed into flow-based features such as packet rate, packet size distribution, inter-arrival time, and connection statistics. Data preprocessing techniques are applied to prepare the dataset for machine learning training. Multiple classification algorithms including Logistic Regression, Support Vector Machine (SVM), K-Nearest Neighbours (KNN), and Random Forest are implemented and evaluated using standard performance metrics such as accuracy, precision, recall, F1-score, and ROC–AUC. Experimental results demonstrate that the Random Forest classifier achieves the highest detection accuracy and provides reliable performance for distinguishing between normal and malicious QUIC traffic patterns. To improve transparency and interpretability of the prediction process, Explainable Artificial Intelligence (XAI) techniques such as SHAP and LIME are incorporated into the framework. These methods highlight the most influential network features contributing to attack detection and help security analysts understand the reasoning behind model predictions. The proposed framework enhances the reliability of encrypted traffic monitoring, improves early detection of QUIC traffic flood attacks, and contributes to strengthening the security of next-generation web communication protocols.

Keywords: QUIC Traffic Analysis, DDoS Detection, HTTP/3 Security, Machine Learning, Random Forest, Explainable Artificial Intelligence, SHAP, LIME, Network Traffic Classification.

I. INTRODUCTION

The rapid growth of internet-based services and cloud applications has significantly increased the demand for secure, reliable, and high-performance communication protocols. Modern web technologies increasingly rely on encrypted protocols such as HTTP/3, which uses the QUIC transport protocol to improve network speed, reduce latency, and enhance user privacy. QUIC operates over UDP and integrates transport and security features, providing faster connection establishment and improved congestion control compared to traditional TCP-based protocols. Due to these advantages, many large-scale web platforms and service providers have

adopted QUIC as the foundation for next-generation web communication systems [1], [2].

Despite its benefits, the adoption of QUIC introduces new challenges for network security and traffic monitoring. One of the major concerns is the detection of Distributed Denial of Service (DDoS) traffic flood attacks targeting HTTP/3 services. In such attacks, malicious sources generate large volumes of requests to overwhelm servers, network infrastructure, or application resources. Since QUIC encrypts a significant portion of transport layer information, traditional network monitoring techniques such as deep packet inspection (DPI) become less effective. As a result, detecting abnormal or malicious traffic patterns in encrypted environments has become increasingly difficult for conventional security systems [3], [4].

Traditional network intrusion detection systems often rely on rule-based detection methods or signature-based approaches. Although these techniques can identify known attack patterns, they struggle to detect emerging threats or previously unseen attack behaviours. Furthermore, rule-based systems require continuous manual updates and may not perform effectively in high-volume network environments. With the increasing complexity and scale of modern network traffic, there is a growing need for intelligent and automated security mechanisms capable of identifying anomalous traffic patterns in real time [5], [6].

Machine learning (ML) techniques have emerged as powerful tools for analysing large-scale network traffic data and detecting security threats. By learning patterns from historical traffic behaviour, ML models can classify network flows as normal or malicious based on statistical and behavioural characteristics. Various machine learning algorithms such as Logistic Regression, Support Vector Machine (SVM), K-Nearest Neighbours (KNN), and Random Forest have demonstrated strong performance in network anomaly detection and intrusion detection systems. These techniques are capable of identifying complex traffic patterns that may indicate potential cyberattacks [7], [8].

However, real-world network datasets present several challenges that can affect model performance. These challenges include high-dimensional feature spaces, noisy or incomplete data, and highly imbalanced class distributions where malicious traffic represents only a small portion of the overall dataset. Without appropriate preprocessing techniques, such issues may lead to biased predictions and reduced detection accuracy. In addition, many advanced machine learning models function as black-box systems, making it difficult for security analysts to understand the reasoning behind their predictions. Lack of interpretability can reduce trust in automated decision-making systems, particularly in critical cybersecurity applications [9], [10].

To overcome these limitations, Explainable Artificial Intelligence (XAI) has gained significant attention in recent research. XAI techniques provide insights into model behaviour by identifying the most influential features contributing to classification decisions. Methods such as SHAP (SHapley Additive Explanations) and LIME (Local Interpretable Model-Agnostic Explanations) allow researchers and security analysts to interpret prediction results and better understand how machine learning models detect malicious network traffic [11], [12].

Motivated by these challenges, this paper proposes a machine learning-based framework for detecting QUIC traffic flood attacks in encrypted HTTP/3

networks. The proposed system analyses flow-level traffic features extracted from captured network data and applies multiple classification algorithms to distinguish between normal and malicious traffic patterns. In addition, explainable AI techniques are integrated to improve model transparency and support interpretability of detection results. The objective of the proposed framework is to achieve reliable and accurate detection of QUIC-based DDoS traffic floods while maintaining model transparency and computational efficiency.

The remainder of this paper is organized as follows. Section II presents the literature survey related to network traffic analysis and machine learning-based intrusion detection systems. Section III discusses the analysis of the existing system and the proposed approach. Section IV describes the system architecture and design methodology. Section V explains the implementation modules of the proposed framework. Section VI presents experimental results and performance evaluation. Finally, Section VII summarizes the conclusions and outlines potential future research directions.

II. LITERATURE SURVEY

Recent advancements in network technologies and cloud-based services have significantly increased the volume of internet traffic and the complexity of network infrastructures. As a result, detecting abnormal network behaviour and cyber threats has become an important research area in cybersecurity. Many researchers have applied machine learning and data-driven approaches to analyse network traffic patterns and identify potential security threats. These techniques are particularly useful in environments where traditional rule-based detection systems struggle to detect evolving or unknown attack patterns [3], [4].

Several studies have explored the use of machine learning algorithms for network intrusion detection and anomaly detection. Sommer and Paxson investigated the application of machine learning techniques in network security systems and highlighted their potential for identifying complex attack patterns within large-scale network traffic datasets. Their study demonstrated that machine learning models can effectively classify malicious activities by learning behavioural characteristics of network flows rather than relying solely on predefined signatures. However, they also emphasized challenges related to feature selection and model interpretability when deploying such systems in real-world environments [5].

To improve the performance of network traffic classification systems, researchers have proposed various feature engineering and data preprocessing techniques. Moore and Zuev analysed internet traffic using statistical flow features such as packet size, inter-arrival time, and connection duration to improve classification accuracy. Their work demonstrated that properly selected traffic features play a crucial role in improving machine learning model performance for network traffic analysis. They also evaluated multiple algorithms, including Decision Trees, Naïve Bayes, and Support Vector Machines, to identify the most suitable models for traffic classification tasks [6].

Ensemble learning approaches have also gained significant attention in the field of network intrusion detection. Breiman introduced the Random Forest algorithm, which combines multiple decision trees to improve prediction accuracy and robustness. Several subsequent studies have applied ensemble-based models such as Random Forest, Gradient Boosting, and AdaBoost to detect distributed denial-of-service (DDoS) attacks and other network anomalies. These

ensemble models typically outperform individual classifiers because they aggregate predictions from multiple weak learners, thereby reducing overfitting and improving detection reliability [7].

With the emergence of modern web protocols such as QUIC and HTTP/3, new challenges have arisen for network monitoring and security analysis. Unlike traditional TCP-based protocols, QUIC encrypts much of its transport-layer information, making it difficult for conventional deep packet inspection (DPI) techniques to analyse traffic contents. Recent studies have investigated the use of machine learning-based traffic analysis to detect anomalies in encrypted network environments. These approaches focus on analysing traffic behaviour through flow-level features rather than inspecting packet payloads, enabling effective detection even when traffic is encrypted [8], [9].

In addition to improving detection accuracy, recent research has emphasized the importance of model interpretability in cybersecurity applications. Many advanced machine learning algorithms function as black-box systems, which can make it difficult for security analysts to understand how predictions are generated. This lack of transparency may reduce trust in automated security systems and limit their adoption in critical infrastructure environments. To address this issue, Explainable Artificial Intelligence (XAI) techniques such as SHAP (SHapley Additive Explanations) and LIME (Local Interpretable Model-Agnostic Explanations) have been proposed to provide interpretable insights into model behaviour [10], [11].

These explainability techniques allow researchers to identify the most influential features contributing to classification outcomes and provide both global and local explanations of model predictions. As a result, XAI enhances transparency, improves system reliability, and helps security professionals better understand how machine learning models detect cyber threats. Integrating explainable AI with machine learning-based intrusion detection systems has therefore become an important direction in modern cybersecurity research [12].

Despite these advancements, several challenges remain in detecting QUIC-based traffic flood attacks in encrypted HTTP/3 environments. Many existing studies focus primarily on traditional network protocols or lack comprehensive approaches that combine high detection accuracy with model interpretability. In addition, issues such as high-dimensional traffic features, dataset imbalance, and the need for efficient real-time detection remain open research problems. Therefore, there is a need for an intelligent and explainable machine learning framework capable of accurately identifying malicious QUIC traffic patterns while maintaining transparency and computational efficiency in next-generation network security systems.

III. SYSTEM ANALYSIS

A. EXISTING SYSTEM

Traditional network security systems mainly rely on rule-based monitoring techniques and signature-based intrusion detection systems to identify malicious activities. These systems analyze network packets using predefined rules or known attack signatures to detect abnormal traffic patterns. While such methods are effective in identifying previously known cyberattacks, they often fail to detect newly emerging threats or sophisticated attack strategies. In addition, maintaining and updating large rule databases requires continuous manual effort, which limits the scalability and adaptability of traditional

security frameworks in modern network environments [5], [6].

With the increasing adoption of encrypted communication protocols such as HTTPS and HTTP/3, traditional packet inspection techniques have become less effective. Modern protocols like QUIC encrypt significant portions of transport-layer information to ensure user privacy and secure communication. Although encryption improves security and data protection, it also reduces network visibility for security monitoring systems. As a result, conventional detection techniques that rely on payload inspection cannot effectively analyse encrypted traffic patterns, making it difficult to identify malicious behaviours such as Distributed Denial of Service (DDoS) traffic floods [7], [8].

To address these challenges, machine learning-based network intrusion detection systems have been introduced in recent years. These systems analyse network traffic behaviour using statistical and flow-level features such as packet size distribution, packet rate, inter-arrival time, and connection duration. Machine learning algorithms including Logistic Regression, Decision Trees, Support Vector Machines (SVM), and Artificial Neural Networks have been widely used to classify network traffic as normal or malicious. These models learn traffic behaviour patterns from historical datasets and apply this knowledge to detect anomalies in real-time network environments [9], [10].

Furthermore, ensemble learning techniques such as Random Forest and Gradient Boosting have been applied to improve detection accuracy and model stability. These algorithms combine predictions from multiple decision trees to generate more reliable results and reduce the risk of overfitting. Ensemble models have demonstrated strong performance in network anomaly detection tasks and have been widely adopted in cybersecurity applications [11].

Recent advancements in network monitoring have also introduced data-driven approaches for analysing encrypted traffic. Instead of inspecting packet contents, these methods focus on analysing traffic behaviour through statistical flow features. By evaluating patterns in traffic volume, connection frequency, and packet timing, researchers have been able to detect abnormal network activities even in encrypted communication environments. However, many existing detection models rely on complex machine learning architectures that often function as black-box systems, making it difficult for security analysts to understand how predictions are generated [12].

To improve transparency and trust in automated security systems, researchers have begun integrating Explainable Artificial Intelligence (XAI) techniques into machine learning-based intrusion detection frameworks. Methods such as SHAP (SHapley Additive Explanations) and LIME (Local Interpretable Model-Agnostic Explanations) are used to interpret model predictions by identifying the most influential features contributing to attack detection. These explainability methods help analysts understand model behaviour and enhance trust in automated cybersecurity solutions [1], [2].

LIMITATIONS OF EXISTING SYSTEM

Traditional rule-based intrusion detection systems are limited in detecting new or unknown cyberattacks, as they rely heavily on predefined attack signatures.

Encryption in modern communication protocols such as QUIC and HTTP/3 reduces network visibility, making it difficult for traditional monitoring systems

to inspect packet contents and detect malicious activities.

Many machine learning-based intrusion detection systems require large volumes of labelled training data, which may not always be available in real-world network environments.

Network traffic datasets often contain high-dimensional features and large volumes of data, which increase computational complexity and training time for machine learning models.

Many advanced machine learning models function as black-box systems, making it difficult for security analysts to interpret model decisions and understand why specific traffic patterns are classified as malicious.

Existing systems often struggle to provide both high detection accuracy and model interpretability simultaneously, which is essential for deploying reliable cybersecurity solutions in real-world network infrastructures.

B. PROPOSED SYSTEM

This section presents the proposed machine learning-based framework designed for detecting QUIC traffic flood attacks in encrypted HTTP/3 networks. The proposed system focuses on analysing network traffic behaviour using flow-based features rather than inspecting packet payloads. By examining statistical characteristics such as packet rate, packet size distribution, connection frequency, and inter-arrival time, the framework can effectively distinguish between normal network activity and malicious traffic patterns.

The proposed framework integrates several components including data preprocessing, feature extraction, machine learning-based classification, and explainable artificial intelligence techniques. During the preprocessing stage, captured network traffic data are transformed into structured datasets containing relevant flow-level features. These features are then used to train multiple machine learning models such as Logistic Regression, Support Vector Machine (SVM), K-Nearest Neighbours (KNN), and Random Forest. Among these models, Random Forest is selected as the primary classifier due to its ability to handle high-dimensional data and provide robust prediction performance.

In addition to improving detection accuracy, the proposed system incorporates Explainable Artificial Intelligence (XAI) techniques such as SHAP and LIME to enhance model interpretability. These methods analyse the contribution of each network feature to the final prediction and provide clear explanations for classification outcomes. This allows network administrators and security analysts to better understand how the model detects QUIC traffic flood attacks and improves trust in the automated detection process.

The main objective of the proposed framework is to achieve reliable detection of encrypted QUIC traffic floods while maintaining high prediction accuracy, transparency, and computational efficiency. By combining machine learning-based anomaly detection with explainable AI techniques, the system aims to strengthen cybersecurity monitoring for next-generation encrypted network environments [1], [2], [8].

IV. SYSTEM DESIGN

SYSTEM ARCHITECTURE

Below diagram depicts the whole system architecture.

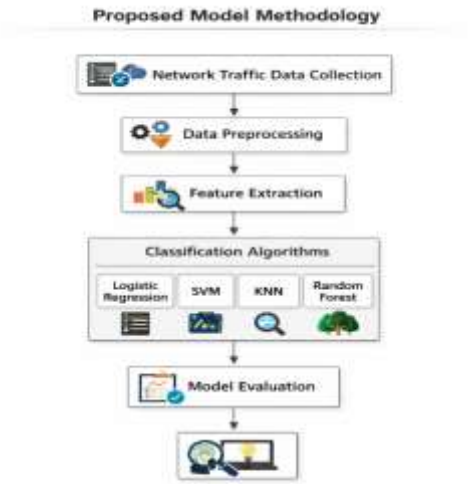

Fig. 1. Methodology followed for proposed model.

Fig 1. Methodology followed for proposed model

V. SYSTEM IMPLEMENTATION

MODULES

This section describes the core implementation modules of the proposed framework for detecting QUIC traffic flood attacks in encrypted HTTP/3 networks. The system is designed as a modular pipeline consisting of traffic data collection, preprocessing, feature extraction, machine learning model training, explainability integration, and prediction evaluation. This modular design improves system scalability, reliability, and interpretability, enabling efficient detection of malicious traffic patterns in modern encrypted network environments.

A. Traffic Data Collection Module

The Traffic Data Collection Module is responsible for capturing network traffic data from the monitored network environment. In the proposed framework, traffic is generated using both normal client behaviour and simulated attack traffic targeting an HTTP/3 server that uses the QUIC protocol.

Network packets are captured using packet monitoring tools and stored in PCAP (Packet Capture) format. The captured traffic includes communication flows between clients and the server operating over UDP port 443, which is commonly used by QUIC-based HTTP/3 communication.

The dataset contains two categories of traffic samples:

• **Normal Traffic:** Generated by legitimate user interactions such as web browsing and service requests.

• **Attack Traffic:** Generated by simulated QUIC traffic flood attacks designed to overwhelm the server with excessive requests.

These traffic samples represent real-world network conditions and provide labelled data required for supervised machine learning training.

B. Data Preprocessing Module

The Data Preprocessing Module prepares the captured traffic dataset for machine learning model training. Network datasets often contain noise, redundant data, and inconsistent traffic samples that may negatively affect model performance if not properly processed.

The preprocessing stage includes the following steps:

Packet Flow Extraction

Captured PCAP files are processed to extract network flows. A network flow represents a sequence of packets exchanged between a source and destination within a specific time interval. Flow-level analysis enables the system to analyse behavioural traffic patterns rather than inspecting encrypted packet payloads.

Feature Generation

From each traffic flow, several statistical features are calculated, including:

- Packet rate (packets per second)
- Byte rate (bytes per second)
- Inter-arrival packet time
- Packet size distribution
- Connection count
- QUIC protocol header features

These flow-level features capture the behavioural characteristics of network traffic and help distinguish normal communication patterns from malicious traffic floods.

Data Cleaning and Normalization

Feature scaling and normalization techniques are applied to ensure consistent feature ranges and remove anomalies in the dataset. This step improves model stability and ensures efficient training of machine learning algorithms.

C. Feature Selection Module

High-dimensional network datasets may contain redundant or less informative features that increase computational complexity and reduce model efficiency. Therefore, a Feature Selection Module is implemented to identify the most relevant traffic features contributing to attack detection.

Feature importance is initially evaluated using tree-based learning algorithms such as Random Forest, which measure the contribution of each feature to classification outcomes. In addition, Explainable AI techniques such as SHAP are used to analyse the importance of network features and rank them based on their influence on model predictions.

By selecting only the most informative features, the framework reduces dataset dimensionality while maintaining detection accuracy. This step decreases computational overhead, accelerates model training, and improves interpretability of the detection system [1], [2], [8].

D. Machine Learning Training Module

The Machine Learning Training Module is responsible for building classification models capable of identifying malicious QUIC traffic patterns. Several machine learning algorithms are implemented and evaluated to determine the most effective model for traffic flood detection.

The evaluated algorithms include:

- Logistic Regression
- Decision Tree
- Support Vector Machine (SVM)
- K-Nearest Neighbours (KNN)
- Random Forest

Each algorithm is trained using the extracted network traffic features. The dataset is divided into training and testing sets to evaluate model performance. Stratified cross-validation is applied to maintain balanced class distribution during training and testing.

Among the evaluated algorithms, the Random Forest classifier demonstrates superior performance due to its ensemble learning structure. By combining multiple decision trees, Random Forest improves prediction accuracy, handles high-dimensional datasets efficiently, and reduces the risk of overfitting [5], [7].

K. Explainability Module (XAI Integration)

To enhance transparency and interpretability, the proposed framework integrates Explainable Artificial Intelligence (XAI) techniques into the detection system. Many machine learning models

operate as black-box systems, which makes it difficult to understand the reasoning behind their predictions. In cybersecurity applications, interpretability is essential for building trust in automated detection systems.

Two XAI techniques are used in the proposed framework:

SHAP (SHapley Additive Explanations): SHAP provides both global and local explanations by quantifying the contribution of each feature to the model's predictions. It helps identify which traffic features have the most influence on detecting QUIC traffic flood attacks.

LIME (Local Interpretable Model-Agnostic Explanations): LIME explains individual predictions by approximating the model behaviour around a specific instance. This allows security analysts to understand why a particular traffic flow is classified as malicious.

These explainability techniques provide valuable insights into model behaviour and assist network administrators in analysing suspicious traffic patterns [1], [2], [8], [12].

E. Prediction and Evaluation Module

The Prediction and Evaluation Module generates the final classification results and evaluates the performance of the trained machine learning models.

The output of the system includes:

- **Traffic Classification Result:** Normal Traffic / QUIC Traffic Flood Attack
- **Prediction Probability Score**
- **Feature Importance Explanations**

To evaluate model performance, several standard metrics are used:

- Accuracy
- Precision
- Recall
- F1-Score
- ROC–AUC Score

These evaluation metrics provide a comprehensive analysis of model performance, particularly in network intrusion detection scenarios where detecting malicious traffic accurately is critical.

By identifying abnormal QUIC traffic behaviour at an early stage, the proposed framework strengthens network security monitoring and helps prevent large-scale Distributed Denial of Service (DDoS) attacks targeting modern HTTP/3-based web services.

VI. RESULTS AND DISCUSSION

This section presents the experimental results and performance evaluation of the proposed machine learning framework for detecting QUIC traffic flood attacks in encrypted HTTP/3 networks. Multiple classification algorithms were implemented and evaluated using a labelled dataset containing both normal traffic and simulated attack traffic. The evaluation focuses on comparing model performance, analysing detection accuracy, and interpreting the contribution of traffic features through explainable AI techniques.

A. Accuracy Comparison of Machine Learning Models

Several machine learning algorithms were evaluated to determine the most effective model for detecting QUIC traffic flood attacks. The models include Logistic Regression, Decision Tree, Support Vector Machine (SVM), K-Nearest Neighbours (KNN), and Random Forest. Model performance was evaluated

using standard classification metrics such as accuracy, precision, recall, and F1-score.

Table 1. Performance Comparison of Machine Learning Models

Model	Accuracy (%)	Precision	Recall	F1-Score
Logistic Regression	88.2	0.86	0.85	0.85
Decision Tree	90.1	0.88	0.87	0.87
Support Vector Machine (SVM)	91.4	0.89	0.88	0.88
K-Nearest Neighbours (KNN)	93.2	0.91	0.90	0.90
Random Forest	95.8	0.94	0.93	0.93

From the comparison results, the Random Forest classifier achieved the highest detection accuracy of 95.8%, outperforming the other models. This superior performance can be attributed to its ensemble learning structure, which combines multiple decision trees to improve prediction stability and reduce the risk of overfitting. Random Forest is also capable of handling high-dimensional traffic datasets and capturing complex behavioural patterns within network flows [5], [7].

B. ROC Curve Analysis

The Receiver Operating Characteristic (ROC) curve is used to evaluate the trade-off between the True Positive Rate (TPR) and False Positive Rate (FPR) for different classification thresholds. The Area Under the ROC Curve (ROC–AUC) is commonly used as a performance indicator for classification models.

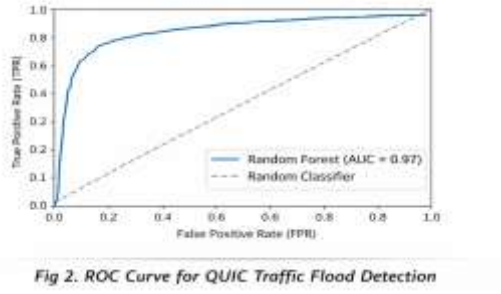

Fig 2. ROC Curve for QUIC Traffic Flood Detection

Fig 2. ROC Curve for QUIC Traffic Flood Detection Model

In this study, the Random Forest classifier achieved a ROC–AUC score of 0.97, indicating excellent classification performance. A ROC curve closer to the top-left corner of the graph represents higher sensitivity and specificity in distinguishing between normal and malicious network traffic.

The ROC analysis demonstrates that the proposed detection framework maintains strong predictive capability even when analysing encrypted QUIC traffic flows. This is particularly important because modern network protocols such as HTTP/3 encrypt most packet contents, making traditional payload inspection techniques ineffective. The proposed machine learning model successfully identifies malicious behaviour using flow-level traffic features instead of inspecting encrypted packet payloads.

C. SHAP Feature Importance Analysis

To improve transparency and interpretability, SHAP (SHapley Additive Explanations) was applied to analyse the contribution of each network feature to the model predictions. SHAP values quantify the influence of individual features on classification outcomes using cooperative game theory principles.

International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

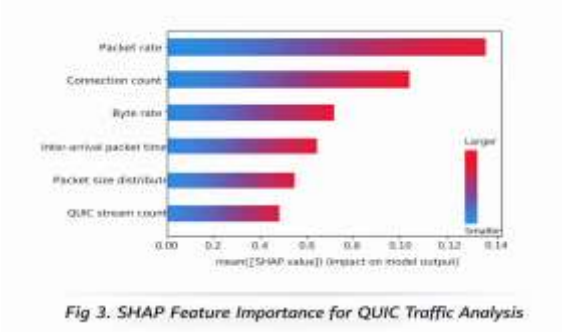

Fig 3. SHAP Feature Importance for QUIC Traffic Analysis

Fig 3. SHAP Feature Importance for QUIC Traffic Analysis

The SHAP analysis revealed that several traffic features significantly influence attack detection. The most influential features include:

• Packet rate (packets per second) • Byte rate (bytes per second) • Inter-arrival packet time • Packet size distribution • Number of network connections

Features with higher SHAP values contribute more significantly to distinguishing malicious traffic floods from normal network communication. For example, abnormal increases in packet rate and connection frequency were strong indicators of QUIC traffic flood attacks.

The global SHAP summary plot illustrates the overall importance of features across the dataset, while local SHAP explanations provide insights into how individual traffic samples influence prediction outcomes.

The integration of SHAP-based explanations enhances the interpretability of the proposed intrusion detection framework. It enables network administrators and cybersecurity analysts to better understand the reasoning behind the model's predictions and verify the reliability of automated attack detection results [1], [2], [8], [12].

V. CONCLUSION AND FUTURE WORK

This study presented a machine learning-based framework for detecting QUIC traffic flood attacks in encrypted HTTP/3 network environments. Modern internet protocols such as QUIC improve performance and security through encryption and faster connection establishment. However, the encrypted nature of QUIC traffic makes traditional packet inspection techniques less effective for detecting malicious activities such as Distributed Denial of Service (DDoS) traffic floods. To address this challenge, the proposed framework analyses network traffic behaviour using flow-level features instead of relying on packet payload inspection.

The dataset used in this study consisted of captured network traffic containing both normal communication flows and simulated QUIC flood attack traffic. Various statistical features such as packet rate, byte rate, inter-arrival time, connection count, and packet size distribution were extracted from the traffic flows to represent network behaviour patterns. Several machine learning models were evaluated, including Logistic Regression, Decision Tree, Support Vector Machine (SVM), K-Nearest Neighbours (KNN), and Random Forest.

Among the evaluated algorithms, the Random Forest classifier achieved the highest detection accuracy and demonstrated strong capability in distinguishing between normal network traffic and malicious QUIC traffic floods. The ensemble learning mechanism of Random Forest allowed the model to handle high-dimensional traffic data effectively while maintaining stable prediction performance and reducing the risk of overfitting [5], [7].

To improve model transparency and interpretability, Explainable Artificial Intelligence (XAI) techniques

such as SHAP and LIME were integrated into the proposed framework. These techniques provided insights into the contribution of individual traffic features to classification outcomes, enabling security analysts to better understand how the model identifies malicious traffic patterns. The integration of explainable AI improves trust, transparency, and reliability of automated intrusion detection systems deployed in modern network infrastructures [1], [2], [8], [12].

Future research can further enhance this work by integrating real-time network traffic monitoring systems and deploying the detection model within cloud-based or edge-based cybersecurity infrastructures. Additionally, advanced deep learning models and hybrid ensemble approaches may be explored to further improve detection accuracy for complex attack patterns. Incorporating adaptive learning mechanisms that continuously update the model using new traffic data can also improve the system's ability to detect evolving cyber threats in next-generation encrypted network environments.

REFERENCES

1. D. Gunning, M. Stefik, J. Choi, T. Miller, S. Stumpf, and G.-Z. Yang, "XAI—Explainable artificial intelligence," Science Robotics, vol. 4, no. 37, 2019, Art. no. eaay7120.
2. A. Barredo Arrieta, N. Díaz-Rodríguez, J. Del Ser, A. Bennetot, S. Tabik, A. Barbado, S. Garcia, S. Gil-Lopez, D. Molina, R. Benjamins, R. Chatila, and F. Herrera, "Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI," Information Fusion, vol. 58, pp. 82–115, Jun. 2020.
3. J. Iyengar and M. Thomson, "QUIC: A UDP-Based multiplexed and secure transport," IETF RFC 9000, May 2021.
4. M. Thomson and S. Turner, "Using TLS to secure QUIC," IETF RFC 9001, May 2021.
5. L. Breiman, "Random forests," Machine Learning, vol. 45, no. 1, pp. 5–32, Oct. 2001.
6. N. Williams, S. Zander, and G. Armitage, "A preliminary performance comparison of five machine learning algorithms for practical IP traffic flow classification," ACM SIGCOMM Computer Communication Review, vol. 36, no. 5, pp. 5–16, 2006.
7. J. Hou, P. Fu, Z. Cao, and A. Xu, "Machine learning based DDoS detection through NetFlow analysis," in Proc. IEEE Military Communications Conf. (MILCOM), 2018, pp. 1–6.
8. A. Adadi and M. Berrada, "Peeking inside the black-box: A survey on explainable artificial intelligence (XAI)," IEEE Access, vol. 6, pp. 52138–52160, 2018.
9. L. Van der Maaten and G. Hinton, "Visualizing data using t-SNE," Journal of Machine Learning Research, vol. 9, pp. 2579–2605, 2008.
10. I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.
11. F. Emmert-Streib, O. Yli-Harja, and M. Dehmer, "Explainable artificial intelligence and machine learning: A reality rooted perspective," WIREs Data Mining and Knowledge Discovery, vol. 10, no. 6, p. e1368, Nov. 2020.
12. A. Holzinger, C. Molnar, P. Biecek, and W. Samek, "Explainable AI methods – A brief overview," in Proc. Int. Workshop Extending Explainable AI Beyond Deep Models and Classifiers, 2020, pp. 13–38.
13. S. Nazat, L. Li, and M. Abdallah, "XAI-ADS: An explainable artificial intelligence framework for enhancing anomaly detection in autonomous driving systems," IEEE Access, vol. 12, pp. 48583–48607, 2024.