International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 01 | Jan 2026 www.irjet.net p-ISSN: 2395-0072

Cyber Threat Detection in Encrypted Traffic Analysis without Decryption

Vaishnavi V, Santhosh Devappa Dubari, Uzma Samreen Madeena

Vaishnavi V, Department of CSE, East Point College of Engineering and Technology, Bengaluru, Karnataka, India
Santhosh Devappa Dubari, Department of CSE, East Point College of Engineering and Technology, Bengaluru, Karnataka, India
Uzma Samreen Madeena, Department of CSE East Point College of Engineering and Technology, Bengaluru, Karnataka, India

---

Abstract - *This paper presents an AI-based cyber threat detection system that analyses encrypted network traffic without the need for decryption. As most modern communication is now encrypted, traditional security systems that rely on payload inspection struggle to identify threats hidden within secure channels. Decrypting traffic introduces computational overhead and privacy risks, making it unsuitable for privacy-focused environments. To overcome this challenge, the proposed system examines traffic metadata such as packet size, flow duration, timing intervals, packet rate, and behavioural patterns instead of inspecting packet contents. A Random Forest machine learning model trained on the CICIDS dataset is employed to classify network flows as normal or malicious, including threats such as DoS, DDoS, Port Scan, Probe, and Brute Force attacks. Live network traffic is captured using Scapy, and the extracted metadata is processed in real time to generate predictions. When abnormal activity is detected, the system immediately triggers alerts and updates an interactive web dashboard developed using Flask and SocketIO, providing visual insights into traffic behaviour, threat severity, and alert logs. Experimental evaluation demonstrates that the proposed approach achieves a* ***detection accuracy of 95%****, outperforming alternative classifiers such as Naive Bayes (86%), KNN (88%), SVM (91%), and Decision Tree (89%). Performance is assessed using standard metrics Including accuracy, precision, recall, F1-score, and detection latency, confirming the system's suitability for real-time deployment in encrypted network environments. By combining AI-driven analysis with real-time visualization and automated alerting, this work offers a lightweight, efficient, and privacy-preserving solution for modern cybersecurity requirements.*

Key Words**: Privacy Preserving Detection, Encrypted Traffic Analysis, No Decryption Approach, Metadata Based Classification, Machine Learning, Random Forest, Cyber Threat Detection, Real Time Monitoring.**

1. INTRODUCTION

Modern network communication relies heavily on encryption to protect user data, but this creates a challenge for traditional security systems that depend on inspecting packet content to identify threats. Since encrypted traffic hides the payload, techniques such as deep packet inspection become ineffective, and decrypting data introduces privacy risks and high processing overhead. As attackers increasingly exploit encrypted channels, there is a growing need for security solutions that can detect malicious activity without accessing sensitive information.

A promising approach is to analyze traffic metadata, such as packet size, flow duration, timing intervals, and packet rate, which reveal behavioral patterns even when the content is encrypted. With the help of machine learning, these patterns can be studied to classify network flows as normal or suspicious. Real time dashboards further support monitoring by presenting alerts and traffic insights in a visual and easy to understand format.

Based on this idea, the proposed system uses AI to detect cyber threats in encrypted traffic without performing decryption. By combining metadata analysis, a trained Random Forest model, live packet capture, and dashboard visualization, the system provides an efficient and privacy preserving solution suitable for modern secure networks.

1.1 Background

Today's digital world depends heavily on online communication, and most of this communication is protected through encryption to keep user information private. While encryption is essential, it creates a major challenge for organizations that need to monitor their networks for harmful activities. When data is hidden inside encrypted traffic, it becomes difficult to understand whether the activity is normal or potentially dangerous. This problem exists because security teams can no longer see what is inside the data being transmitted, yet attacks still happen through the same encrypted channels. As a result, users, companies, and

online services are all affected, since threats can spread without being easily noticed. With cyberattacks increasing every year and more services moving online, the need to identify suspicious behavior in encrypted communication has become more important than ever. A reliable way to detect harmful activity without violating user privacy is now a critical requirement for modern network security.

1.2 Problem Statement

Modern network traffic is heavily encrypted, making traditional security systems unable to inspect data and detect hidden threats. Existing methods that rely on reading packet content fail under encryption and create privacy concerns. As attackers exploit this gap, there is a growing need for a new approach that can identify suspicious activity in encrypted traffic without breaking user privacy.

1.3 Objectives

- To design and develop a system that can detect cyber threats hidden within encrypted network traffic without performing any form of decryption, by focusing entirely on metadata such as packet size, timing behavior, and flow characteristics, allowing the system to identify abnormal traffic patterns with measurable accuracy while maintaining user privacy.

- To classify network activity into normal and suspicious categories in real time, enabling the detection of major cyberattacks such as DoS, DDoS, Port Scanning, and Brute Force attempts, and ensuring that harmful behavior is recognized at the earliest possible stage for timely intervention.

- To build an automated and intelligent web based dashboard that provides clear visualization of alerts, live traffic summaries, and monitoring results, helping users interpret network behavior quickly, improving situational awareness, and supporting faster and more informed security decisions.

- To improve the overall speed, reliability, and efficiency of threat detection by minimizing manual effort and avoiding heavy data processing, ensuring that the system functions as a lightweight, scalable, and privacy preserving solution suitable for modern encrypted network environments.

1.4 Scope of the System

The system is designed to be used in environments where encrypted network communication is common, including educational institutions, corporate networks, data centers, and internet service platforms. It can be used by network administrators, cybersecurity teams, and organizations seeking privacy preserving threat detection. The system monitors real time traffic behavior, helping users identify unusual activity without exposing sensitive data. While it focuses on major threats such as DoS and Port Scanning, future versions may expand to handle more complex attack types and larger network scales. The system can also be integrated into existing security workflows to improve visibility in encrypted environments. Its real world usability lies in offering a lightweight, automated, and privacy focused approach to threat monitoring that adapts to modern security needs.

2. Literature Survey

1. AI Driven Encrypted Traffic Threat Detection– 2024

Researchers in this study explore how cyberattacks can be identified within SSL and TLS encrypted communication without accessing the actual payload. Their work shows that machine learning models can recognize unusual behavior by examining metadata trends such as timing, flow duration, and packet size. The findings suggest strong potential for privacy friendly threat detection. However, the study focuses mainly on experimental results and does not address real time deployment or integration with monitoring tools.

2. Privacy Preserving Intrusion Detection Using Flow Based Features – 2024

This work investigates the use of flow level characteristics to detect malicious traffic while completely avoiding packet content inspection. Techniques such as gradient boosted models and deep learning are used to classify encrypted flows more accurately than traditional systems. Although the approach protects user privacy, it is mostly tested offline and does not include a simple mechanism for live alerting or operational use in practical environments.

3. MPAF: Encrypted Traffic Classification with Multi-Phase Feature Extraction – 2024

This work proposes a multi-phase encrypted traffic classification framework that extracts behavioural and temporal metadata features from network flows without decrypting packet payloads. By analysing traffic patterns at different phases of a session, the approach improves detection accuracy compared to traditional single-stage methods. Although the framework demonstrates strong classification performance on benchmark datasets, it primarily focuses on offline analysis and does not integrate real-time visualization dashboards or automated mitigation mechanisms, which limits its applicability in operational security environments.

4. Real Time Cyber Threat Monitoring with Web Dashboards – 2025

This study highlights how visualization tools can support cybersecurity analysts by presenting alerts, summaries, and AI generated insights in real time. Dashboards help users quickly understand ongoing network behavior and respond to threats faster. Even so, most existing dashboards remain separate from encrypted traffic detection engines and do not provide a unified end to end system.

5. Machine Learning for Encrypted Network Traffic Analysis – IEEE Survey

This survey reviews machine-learning techniques for analysing encrypted traffic using payload-independent features such as packet size, flow statistics, timing intervals, and traffic direction. The authors emphasize that ensemble models, including Random Forest, often achieve a strong balance between accuracy and computational efficiency for practical deployments. The study also discusses challenges related to real-time deployment, false-positive reduction, and system integration, highlighting the need for unified solutions that combine detection, visualization, and automated response—objectives addressed by the proposed system in this work.

2.1 Existing Cyber Threat Detection Techniques

Traditional cyber threat detection techniques primarily rely on examining the actual content of network packets to identify malicious patterns. The most widely used approach is signature based detection, where the system compares incoming traffic with a database of known attack signatures. While effective for familiar threats, it struggles with new or evolving attacks that do not match existing patterns. Another common method is deep packet inspection, which scans packet payloads to detect harmful behavior. However, this technique becomes ineffective when traffic is encrypted, since the system cannot view the hidden content.

Some tools use rule based detection, where analysts manually create rules for suspicious behavior, but these systems require constant updates and expert involvement. Anomaly based detection attempts to flag unusual patterns, yet it often produces false alarms and may misinterpret legitimate traffic as dangerous. As encryption becomes the default across networks, these traditional techniques face increasing limitations, making it difficult for organizations to monitor threats without compromising user privacy or system performance.

2.2 Limitations in Traditional Monitoring Systems

Traditional network monitoring systems depend heavily on inspecting packet content to identify threats, which becomes ineffective when traffic is encrypted. These systems cannot access hidden payloads, leaving a large blind spot that attackers often exploit. They also require frequent rule updates and manual tuning, making them slow to adapt to new or unknown attacks. Deep packet inspection introduces privacy concerns and increases processing overhead, which limits real time performance. Many traditional tools detect threats only after an attack has already occurred, reducing their usefulness in fast moving network environments. As encryption becomes more widespread, these limitations prevent conventional monitoring systems from providing accurate, reliable, and privacy conscious protection.

2.3 Research Gap Identification

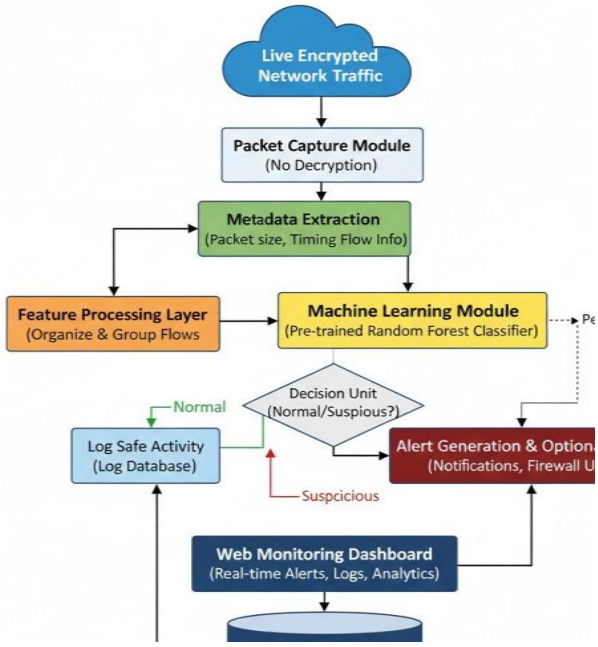
Although several studies explore detecting threats in encrypted traffic using metadata and machine learning, most existing approaches are limited to offline experiments and do not provide real time monitoring capabilities. Many systems lack an integrated dashboard for visualizing alerts or supporting quick decision making, which reduces their practical usability. Current techniques also rely on complex or computationally heavy models that are difficult to deploy in lightweight environments. Additionally, very few solutions offer end to end automation, where traffic is captured, analyzed, classified, and alerted without manual intervention. There remains a clear gap for a privacy preserving, real time, easy to deploy system that can accurately detect threats inside

encrypted communication while presenting results through a user friendly interface.

3. System Architecture

The system uses a real-time processing pipeline where encrypted network traffic is captured and transformed into metadata for analysis. Relevant features are extracted and fed into a machine learning model that classifies each network flow as normal or suspicious. Based on this decision, the system either logs the activity or raises alerts. These alerts are visualized on a web dashboard for continuous monitoring. This approach preserves user privacy while enabling fast and accurate threat detection.

3.1 Overall System Design



4. Methodology

4.1 Data Collection:

The system uses two primary sources of data to support both model training and real time detection. For offline training, the CICIDS dataset is used, which provides a large collection of labeled network flows containing normal traffic and various cyberattacks such as DoS, DDoS, Port Scan, and Brute Force. This dataset offers rich metadata features that help the model learn behavioral differences between legitimate and malicious traffic. For real time operation, live network packets are captured directly from the system's network interface. These captured packets contain encrypted traffic, and only metadata such as packet size, timestamps, and flow direction is extracted. By combining a benchmark dataset for model learning with live traffic for monitoring, the system ensures both accurate classification and practical deployment in real world environments.

4.2 Data preprocessing :

Data preprocessing is performed to convert raw network traffic into a clean and structured format suitable for machine learning analysis. The encrypted packets captured from the network contain only metadata, so the system organizes this information into flow-based records by grouping packets that share the same source, destination, and protocol. Missing or inconsistent values are handled, and numerical fields such as packet size, inter-arrival time, and flow duration are standardized to maintain uniformity. The metadata is then transformed into feature vectors that align with the structure used during model training. This step ensures that both training data from the CICIDS dataset and live traffic follow the same format, allowing the classifier to make accurate predictions. Proper preprocessing improves model performance, reduces noise, and ensures reliable real time detection.

4.3 Feature Extraction :

Feature extraction focuses on converting raw encrypted traffic into meaningful behavioral indicators that can be analyzed by the machine learning model. Since the payload cannot be inspected, the system extracts only metadata from each packet, including packet size, timestamp, flow direction, and protocol information. These packet-level details are then aggregated into flow-based features such as total packets, average packet size, flow duration, packet rate, and inter-arrival time statistics. These features capture how a device behaves on the network rather than what data it transmits, making them suitable for privacy-preserving analysis. The extracted features are aligned with the structure used in the CICIDS dataset to maintain consistency during training and detection. This step ensures the model receives accurate and standardized input that reflects real-world traffic behavior, enabling effective separation of normal and suspicious network flows.

4.4 Machine Learning:

The machine learning component forms the core of the system's threat detection capability. A Random Forest classifier is selected due to its stability, high accuracy, and ability to handle complex network behavior patterns. The model is trained using the CICIDS dataset, which contains

labeled examples of both normal traffic and various cyberattacks. During training, the model learns to distinguish malicious flows by recognizing unique patterns in metadata-based features such as packet rates, flow durations, and size variations. Once trained, the model is deployed in real time to evaluate incoming traffic. Each processed feature vector from live flows is fed into the classifier, which predicts whether the flow represents normal activity or a potential threat. This approach enables fast, automated decision-making without inspecting packet content, making the system effective even when traffic is fully encrypted.

4.5 Threat Classification and Alert System :

After the machine learning model evaluates a flow, the system classifies the activity as either normal or suspicious based on the predicted threat level. This classification is performed in real time, allowing the system to identify attacks such as DoS, DDoS, Port Scanning, Probe attempts, or Brute Force activity as soon as abnormal behavior is detected. Once a flow is labelled as malicious, the alert system is automatically triggered. The system generates an instant warning message and sends it to the user through integrated notification channels, such as a web dashboard or messaging service. At the same time, the dashboard updates to display the detected threat, its source, and the associated confidence score. The alert system may also initiate automated actions, such as temporarily blocking the suspicious IP address to prevent further damage. This combined classification and alert mechanism ensures fast, accurate detection and immediate response, supporting continuous monitoring in encrypted network environments.

4.6 Auto-Blocking Mechanism

The proposed system incorporates an automated IP blocking mechanism that provides immediate mitigation against detected cyber threats in real time. After a network flow is classified by the machine learning model, the associated prediction confidence is evaluated against a predefined threat threshold, and flows identified as malicious trigger an automatic containment response. The source IP address is dynamically blocked through firewall rule enforcement, preventing subsequent packets from reaching protected services. To minimize false blocking and operational disruption, the mechanism includes safeguard checks such as allow-listed trusted addresses and exclusion of private network ranges. All blocking actions are recorded with timestamps, predicted attack categories, and confidence scores for auditing and forensic analysis, while the integrated dashboard visualizes these responses instantaneously. This automated and controlled response framework significantly reduces reaction time to active attacks and strengthens overall network security posture.

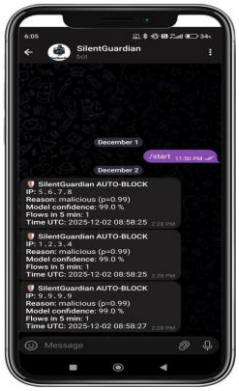
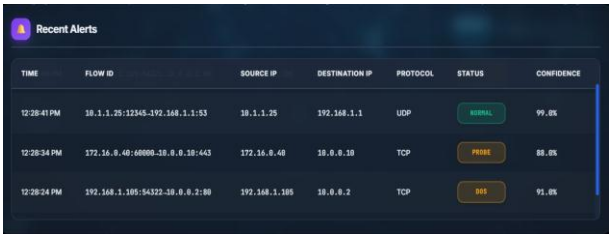


Fig 4.5.1: Alert System through Telegram.

Pseudo-code:

```
BEGIN

Capture incoming network packet
Extract packet and flow features  Send
features to trained ML model

Receive predicted_label and probability

IF predicted_label = "Malicious" OR probability ≥  Threshold
THEN

  IF source_ip NOT IN Allowlist AND source_ip IS NOT  Private_IP
THEN

    IF source_ip NOT IN Recently_Blocked_List THEN  Generate
      firewall rule to block source_ip

      Store source_ip, timestamp, and reason in database  Add
      source_ip to Recently_Blocked_List

    END IF
  END IF
```

Alerts



6. Results and Discussion

6.1 Algorithm Performance Comparison

To justify the selection of an appropriate machine learning model for intrusion detection, a comparative analysis was conducted among multiple classification algorithms. The performance of Naive Bayes, K-Nearest Neighbors (KNN), Support Vector Machine (SVM), Decision Tree, and Random Forest was evaluated based on detection accuracy using the same dataset and feature set. This comparison helps in identifying the most effective algorithm for real-time intrusion detection and prevention.

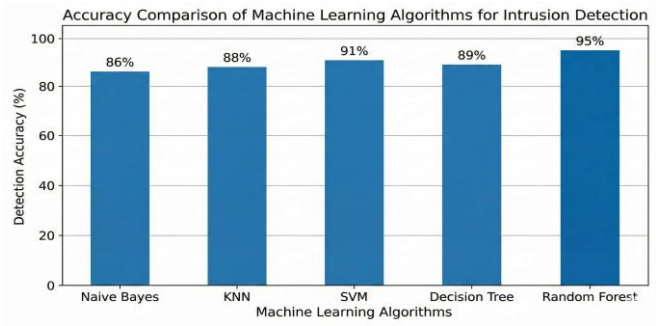


Fig: 6.1 Accuracy Comparison of Machine Learning

Algorithms for Intrusion Detection

Fig. 6,1 presents the accuracy comparison of various machine learning algorithms used for intrusion detection. Among the evaluated models, the Random Forest classifier achieves the highest detection accuracy of 95%, outperforming Naive Bayes, KNN, SVM, and Decision Tree algorithms. The improved performance of Random Forest can be attributed to its ensemble learning approach, which combines multiple decision trees to reduce overfitting and enhance generalization. Additionally, Random Forest efficiently handles high-dimensional network traffic data and noisy features, making it highly suitable for real-time intrusion detection systems. Based on this comparative analysis, Random Forest was selected as the core classification model for the proposed system.

6.2 Classification Performance Evaluation

The proposed Random Forest-based intrusion detection system was evaluated using a merged dataset comprising approximately **2.83 million network flow records** collected from multiple traffic scenarios, including benign activity and diverse attack types such as DDoS, DoS variants, Port Scan, brute-force attacks, and web-based exploits. A subset of six statistically significant flow-level features—Destination Port, Flow Duration, Total Forward Packets, Total Backward Packets, Flow Bytes/s, and Flow Packets/s—was used for training and testing after preprocessing.

The experimental results demonstrate an **overall detection accuracy of 99.45%**, highlighting the strong discriminative capability of the proposed approach even when operating solely on traffic metadata. As shown in the confusion matrix, the classifier achieves near-perfect recognition of major attack categories such as DDoS, DoS Hulk, Port Scan, FTP-Patator, and benign traffic, each attaining precision and recall values close to unity.

However, comparatively lower performance is observed for rare classes such as Web Attack–Brute Force, Web Attack–SQL Injection, and Web Attack–XSS due to severe class imbalance in the dataset. Despite this, the weighted average F1-score remains **0.99**, confirming that the system maintains robust performance across large-scale traffic conditions. These results indicate that the proposed metadata-driven Random Forest model is highly effective for real-time cyber-threat detection in encrypted network environments.

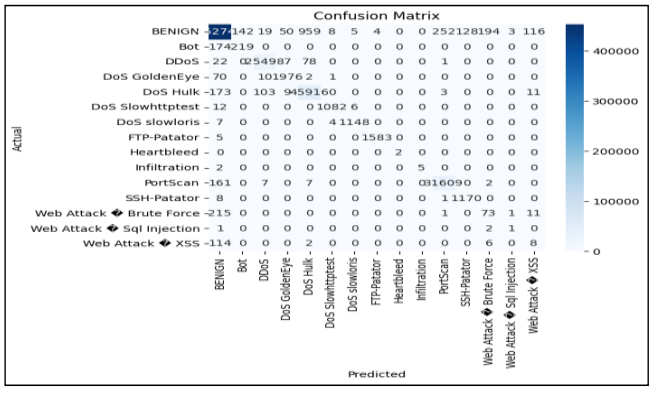


Fig. 6.2: Confusion Matrix for Multi-Class Intrusion Detection Using Random Forest

Conclusions

The proposed system demonstrates an effective approach for detecting cyber threats in encrypted network traffic without relying on packet decryption. By focusing on metadata analysis and machine learning, the system is able to identify abnormal behavior while preserving user privacy and avoiding the overhead of traditional inspection methods. Real time classification, automated alerting, and an interactive dashboard provide continuous visibility into network activity, allowing users to respond quickly to suspicious events. The combination of live monitoring and a trained Random Forest model ensures reliable detection across multiple attack types. Overall, the system offers a modern, lightweight, and practical solution that enhances network security in environments where encryption is widely used, and it lays the groundwork for further improvements in intelligent, privacy-conscious threat detection.

Acknowledgement

It gives us immense pleasure to express our deep sense of gratitude to Dr. Pradipkumar Dixit, Principal, East Point College of Engineering and Technology, Bengaluru, for his constant encouragement and support throughout the duration of this work. We would also like to extend our sincere gratitude to Dr. I. Manimozhi, Head of the Department, Department of Computer Science and Engineering, EPCET, for her continuous guidance, motivation, and valuable suggestions during the course of this project. We are truly thankful to our guide, Mrs. Madhu Shree R, for her expert mentorship, patience, and insightful feedback, which greatly contributed to the successful completion of our project. We also appreciate the support of all faculty members, staff, and our peers who helped us directly or indirectly. Their cooperation and encouragement made this work possible.

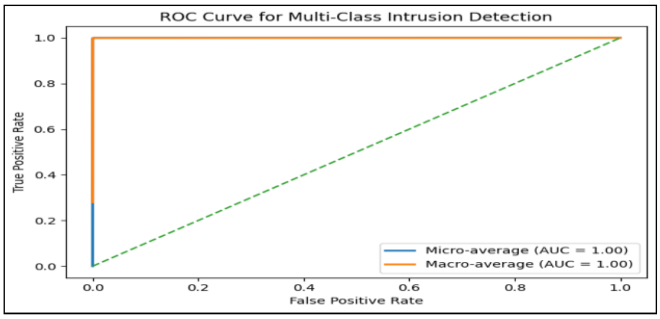


Fig. X: Micro- and Macro-Average ROC Curves for Multi-Class Intrusion Detection

Fig. 6.3 illustrates the receiver operating characteristic (ROC) curves obtained for the proposed Random Forest-based intrusion detection system. Both micro-average and macro-average ROC curves achieve an area under the curve (AUC) of 1.00, indicating excellent class separability and highly reliable discrimination between benign and malicious network flows. The near-perfect ROC performance demonstrates the effectiveness of metadata-driven feature extraction combined with ensemble learning for encrypted traffic analysis. These results further confirm the suitability of the proposed system for real-time cyber-threat monitoring and prevention.

5. References

[1] B. Anderson and D. McGrew, "Identifying encrypted malware traffic with contextual flow data," in Proc. ACM Internet Measurement Conf. (IMC), 2016, pp. 1–14.

[2] M. Shafiq, X. Yu, and D. Li, "Encrypted traffic classification using machine learning: A survey," IEEE Commun. Surveys Tuts., vol. 22, no. 3, pp. 1881–1906, 2020.

[3] M. Lotfollahi, M. J. Siavoshani, R. S. Moshkenani, and M. Saberian, "Deep packet: A novel approach for encrypted traffic classification using deep learning," IEEE Trans. Netw. Sci. Eng., vol. 5, no. 2, pp. 1–13, 2018.

[4] G. Aceto, D. Ciuonzo, A. Montieri, and A. Pescapé, "Mobile encrypted traffic classification using deep learning," Comput. Netw., vol. 154, pp. 1–13, 2019.

[5] Canadian Institute for Cybersecurity, "CICIDS 2018: Intrusion detection evaluation dataset," Univ. of New Brunswick, Fredericton, NB, Canada, 2018.

[6] I. A. Alwhbi, C. C. Zou, and R. N. Alharbi, "Encrypted network traffic analysis and classification utilizing machine learning," Sensors, vol. 24, no. 3, pp. 1–18, 2024.

[7] T. Xu, H. Zhang, and F. Li, "Feature mining for encrypted malicious traffic detection using deep learning," arXiv preprint, 2023.

[8] A. Mareedu, "Machine learning for secure network traffic analysis: From flow classification to encrypted threat detection," ESP-IJACT, 2025.

[9] E. C. Neto, S. Iqbal, and S. Buffett, "Deep learning for intrusion detection in emerging networks: A comprehensive review," arXiv preprint, 2025.

[10] R. Alshammari and N. Zaman, "Encrypted network traffic classification based on machine learning," Ain Shams Eng. J., vol. 15, no. 1, pp. 1–14, 2024.