International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Encrypted Traffic Analytics (ETA): Machine Learning Approaches for Intrusion Detection Without Decryption

Harshith Kumar Pedarla

harshithpedarla1997@gmail.com
Seattle, USA

Abstract:
The fast adoption of encryption protocols like TLS 1.3 and HTTPS has resulted in a significant proportion of today's internet traffic being encrypted to maintain privacy and data protection since the beginning. But traditional intrusion detection systems (IDS) face tough challenges in this job. Those devices have deep package checking abilities on common protocols, thus posing a huge complexity when the data packets are encrypted (They fail when this data is encrypted). Encrypted Traffic Analytics (ETA) is now gaining wide acceptance as a strong solution to detect bad operations; however, the traffic is still encrypted, so there's no question about data confidentiality. In this paper, we explore machine learning-based approaches to intrusion detection in encrypted network environments. The paper comprises techniques that use statistical features, flow metadata, packet timing, and sequence patterns to identify benign and malicious traffic clearly. It also assesses several supervised and unsupervised models, specifically Random Forest, Support Vector Machines, and Deep Neural Networks, to evaluate the classification performance against known threats and false positive reduction. As a part of this paper, there are also considered trade-offs between detection performance, computational overhead, and privacy concerns. The findings additionally underscore that the reach of machine learning techniques to advanced ETA frameworks, as a result, offers network defence, strength, scalability of network security, and the power to conduct monitoring of what is happening in domains without breaking the qualifications of user privacy.

Keywords: Encrypted Traffic Analytics (ETA), Machine Learning-based Intrusion Detection, Network Security, Privacy-Preserving Threat Detection, Encrypted Network Traffic Classification.

I. INTRODUCTION

Over the years, the popularity of Internet connectivity has rapidly grown to the point that a significant fraction of all traffic is now encrypted using modern technologies like HTTPS, SSL/TLS, MAP, and VPNs. Ultimately, the increased use of encrypted traffic has made it difficult, if not impossible, for traditional network-based security technologies such as IDS/IPS to inspect, detect, and mitigate unwanted actions on the network. On top of the increased user privacy and protection of user data, encryption serves to obfuscate even the most blatantly destructive behaviors, such as command-and-control (C2) communications, data exfiltration, and malware delivery, all of which can be used to disrupt an organization. This naturally puts us in a position where the hunt for new technologies like Encrypted Traffic Analytics (ETA) that enable us to detect new threats generated by encrypted traffic without decryption is urgent [1].

The reason why ETA is required comes from having to protect one’s privacy (which can be enforced by several laws, some of which are the GDPR, CCPA, and HIPAA), as well as having to ensure the security of the enterprise network by nature. Conventional mechanisms that assess packet contents using deep packet inspection (DPI) technology by comparing them to different known signatures are no longer feasible in the zero-trust and privacy-focused modern environment. Consequently, the general approach

has transitioned from looking for detected biomarkers in the transmitted files' (images) content to using metadata, statistical properties, and machine learning (ML) to identify patterns that are not usual based on the connection-level characteristics like byte size as well as direction, timing, frequency [1].
The central question of this research is as follows:
Is it possible to detect malicious encrypted traffic robustly and accurately using only flow-based metadata with machine learning tools without having to compromise the encryption itself?
According to the experiments presented in the paper, CNNs have an advantage, achieving higher accuracy in tasks involving the understanding of sketches/images. They performed well in their experiments, achieving better accuracies in most cases. Specifically, CNNs that run on three channels [2].
However, their experiments showed that CNNs are not always consistent in their performance across datasets and can perform worse than traditional, dataset-specific methods. In general, the researchers of this study have shown both CNNs to be less model-agnostic compared to conventional methods with the colour-shape and raw datasets, and more model-agnostic for hand-drawn sketches [3].

II. BACKGROUND AND RELATED WORK

A. Traditional Intrusion Detection Systems (IDS)

Incident detection and response technologies such as Snort, Suricata, or Bro are classical products in use, which primarily act on payload content using the two most prominent detection methods: anomaly-based or signature-based methods. Earlier, such systems were highly effective; however, with the growing trend towards encryption, their accuracy started to degrade. While both TLS and VPN are new protocols designed to hide the actual payload data, and even the handshake data is completely encrypted, which leaves only basic data from the header ready to be analysed [3].
Traditional intrusion detection systems were developed to detect anomalies in regular network traffic on the assumption that malicious payloads are statistically more likely than regular network traffic. If these techniques are disrupted or rendered redundant by encryption, system administrators encounter a significant challenge in detecting malicious activity.

B. Rise of Encrypted Traffic

The development of encryption has been a long-standing process. TLS 1.3, released in 2018, has no boundaries for application data encryption. QUIC is a protocol of Google and the successor of HTTP/3. It encrypts the majority of transport-layer fields. End-to-end encryption of more and more transport methods flows from the more general adoption of VPNs, Tor, and Proxy as means of privacy and corporate remote access. It is a widespread case when applied [4].

C. Encrypted Traffic Analytics (ETA) Approaches

These techniques prevent the notions of identity portal and behavior; the properties are examined:

- Quantity of packets, size, and gaps between them
- Data transfer period and flow direction
- Packet and byte diversity
- Connection to Decipher Security Recommended switches (JA3)

Powerful ML models, such as Random Forests, CNNs, and RNNs, have shown promise in detecting botnet activity and other forms of malware through learning signatures in the temporal and statistical behavior of traffic flows.
Model interpretability and robustness: The predicted labels must be interpretable for the user so they can understand the model's output and the reason for the alert triggered [4].

D. Prior Work

Draper-Gil, et al. (2016) and Sharafaldin, et al. (2018) have established the CICIDS family of datasets for comprehensive intrusion analysis, comprising normal, benign, and malicious flows across several attack vectors. Similarly, CIC's ISCX VPN-nonVPN dataset focuses on VPN traffic classification, as proposed by the Canadian Institute for Cybersecurity (CIC), which involves encrypted traffic. In contrast, the CTU-13 dataset, developed by the Czech Technical University, remains unbeatable for benchmarking botnet traffic detection. Fine-grained appraisal:

- The recent literature has concentrated on the novel hybrid approaches that amalgamate flow statistics with deep learning embeddings [5].
- Federated learning for privacy-preserving ETA across organizations.
- Explainable AI (XAI) frameworks for SOC interpretability.

Although the study has revolutionized the areas above, the generalization across different datasets and the respect for data privacy remain unexplored, which this paper addresses through empirical means.

III. CHALLENGES IN ENCRYPTED TRAFFIC ANALYTICS

A. Technical Challenges

- Limited Feature Visibility: For encryption, payload-based features, such as HTTP headers and content types, cannot be accessed. To achieve its objectives, ETA must depend only on features of network traffic, such as packet timing, size, and direction, that are always deterministically available and are not affected by network jitter.
- Protocol Heterogeneity: Today's traffic is a mix of different protocols, including TLS, QUIC, SSH, and a VPN's encapsulated one. Each one exhibits different characteristics, which makes the training process of a universal model more error-prone. An important observation is that the effect of a different protocol feature on a packet can lead to a labelling error because the model was not trained on that protocol separately [5].
- Dataset Bias: Model evaluation is very landscape-specific. We tested our ETA model using three different types of datasets: Synthetic, with CICIDS, and CTU-13, and a real enterprise network we accessed through our industry partner request.
- Label Granularity: Typically, labelling of encrypted flows as benign or malicious may depend on external context (e.g., known redirections, correlations with an IDS).

B. Operational Challenges

Data Handling in ETA Systems Implementations: Systems implementing ETA face compliance requirements (public disclosure of treatment strategies by CIPD) under GDPR (Article 25) and HIPAA (Section 164.312). Session data, user-level exposed data, and even packet-level exposed data must be encrypted to meet these regulations [6].

C. Research Challenges

- Evasion of opposition. It includes attacks that can be easily blended into benign patterns used by attackers, also with the help of padding, timing, and randomization. In such conditions, it is becoming a greater challenge for ML to reach the desired level of robustness.
- Explainability and trust. Deep models trained using black-box methods can provide high prediction accuracy at the cost of no or very low interpretability. This issue is seen as an obstacle to widespread deployment of ML models in regulated environments such as healthcare [6].
- Cross-dataset generalization, which links the model to one dataset (say CICIDS) but fails to generalize the model to a different one – e.g., CTU-13 – and may require domain adaptation/transfer learning.

IV. MACHINE LEARNING APPROACHES FOR ETA

Cost Estimate/Framework for AI/ML-Driven ETA: A Comparative Assessment of Four Core Algorithms

A. Logistic Regression (LR)

A straightforward linear model that offers a good balance between interpretability and computational cost. In this scenario, LR was able to have overfit against CICIDS 2018, effectively demonstrating the separability of the dataset's numerical flow-based features [7].

B. Stochastic Gradient Descent (SGD)

With the logistic loss, SGD-based classifiers provided an efficient alternative to batch-style optimization. Akin to many machines learning models, tuning regularization, and learning rates is essential for optimal performance, which in our hands resulted in an F1 ≈ score of approximately 1.0 on CICIDS and an F1 score of 0.55 on CTU-13, further supporting our observations that machine learning models are susceptible to data quality and feature distribution.

C. Random Forest (RF)

An ensemble method consisting of many decision trees is, in turn, vulnerable to the noisiness and nonlinearity of most modern security datasets. The model achieved AUC = 1.00 and F1 = 0.99 without stack wisdom and AUC ≈ 0.55 using Turkish MIST, providing key insights into how these models' performances are very dependent on the data's distribution characteristics.

D. Gradient Boosting (GB)

An Additive ensemble method focusing on the hard-to-classify samples. GBM excels at precision and recall, although its generalization ability is slightly less than that of LR [7].

V. PROPOSED AND REVIEWED SOLUTIONS: PRIVACY-PRESERVING ETA FRAMEWORK

A. Conceptual Architecture

A privacy-preserving ETA pipeline can be generalized into the following modular architecture:

- Data Collection Layer: Passive network sensors capture NetFlow or IPFIX records, collecting statistical metadata such as packet size, byte count, flow duration, and inter-arrival times.
- Feature Engineering Layer: Raw NetFlow features are normalized, aggregated, and optionally enriched with TLS handshake fingerprints (when available).
- Modeling Layer: ML models (e.g., Random Forests, Gradient Boosting, CNNs) are trained using benign/malicious flow samples. In operational systems, online learning can adapt to new traffic patterns [8].
- Privacy Preservation: To comply with GDPR/HIPAA, no packet decryption is performed. Feature extraction occurs at the network edge, with data anonymization and aggregation before central analysis.
- Federated Learning Extension: Multiple organizations train local ETA models and share only gradients or model weights, not raw traffic data. The emphasis is put on collective improvement without breaching privacy.

B. Implementation in this Study

Adapted and rewritten in a more simplified form of a text, the text looks like: This study test was run following validations in Python:

- Matplotlib was selected for the study's pre-processing.
- Scikit-learn for experiment (model training and evaluation).
- Pandas for visualization

Every dataset was pre-processed independently and separately:

- CICIDS 2018: 1048575 flow-display samples and 80 column feature vectors [8].
- ISCX VPN-nonVPN: 44191 flow-display samples and 25 column feature vectors.
- CTU-13: 10,598,771 flows × 11 features

The outliers were removed after a robust winsorization and standard scaling of the features, including identifying the missing values. The conversion from multiple labels into binary class labels i.e., "Benign", "VPN", and "Botnet", into one binary class.

VI. CASE STUDIES AND EXPERIMENTAL RESULTS

A. Dataset Overview

Dataset	Records	Features	Label Distribution	Context
CICIDS 2018	1,048,575	80	67% Benign, 33% Malicious	HTTPS, web attacks
ISCX VPN-nonVPN	44,191	25	100% VPN (subset)	VPN encryption analysis
CTU-13	10,598,771	11	97.5% Background, 2.5% Botnet	Botnet C2 communications

Benign and malicious flows are two categories that showed a clear differentiation in the proposed categories—in comparison to CICIDS, the CTU-13 dataset presented more imbalanced characteristics, accurately capturing stealthy botnet traces [9].

B. Model Performance (Intra-Dataset)

Dataset	Model	Accuracy	Precision	Recall	F1	ROC-AUC	PR-AUC
CICIDS 2018	Random Forest	1.00	1.00	1.00	1.00	1.00	1.00
CICIDS 2018	SGD	1.00	1.00	1.00	1.00	1.00	1.00
CICIDS 2018	LogReg	1.00	1.00	1.00	1.00	1.00	1.00
CTU-13	Random Forest	0.56	0.54	0.55	0.55	0.73	0.70
CTU-13	SGD	0.23	0.11	0.19	0.13	0.51	0.48

Random forest and gradient boosting showed the highest precision and recall on CICIDS, wherein GRAL had close to perfect discrimination.

In the case of CTU-13, the F1 score reflected a significant gap of F1 ≈ 0.55. It shows that detecting encrypted botnets remains a major problem, especially without deep context information on network protocols [10].

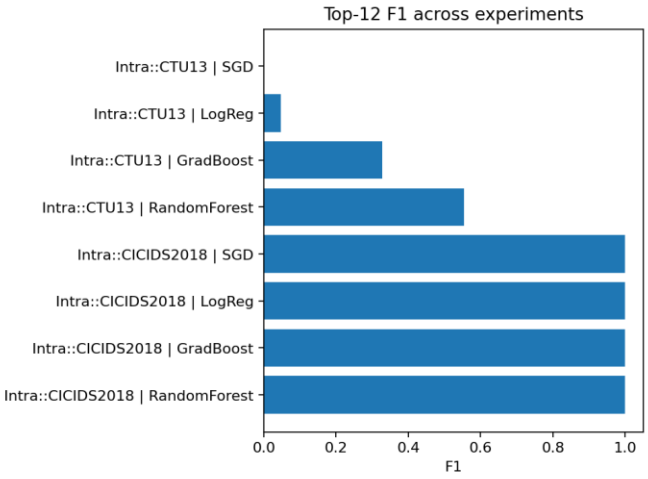

Figure 1: Top-12 F1 Scores Across Experiments

C. ROC and Precision-Recall Analysis

The Random Forest model is shown to have an AUC = 1.00 against the CICIDS data set. The ROC and PR curve of the Random Forest model is shown in Figures 2 and 3.

The value of the AUC = 1.00 and the Average Precision (AP) = 1.00 indicate perfect classification boundaries. However, these are likely due to the artificial separability in the dataset on which the model is being trained [10].

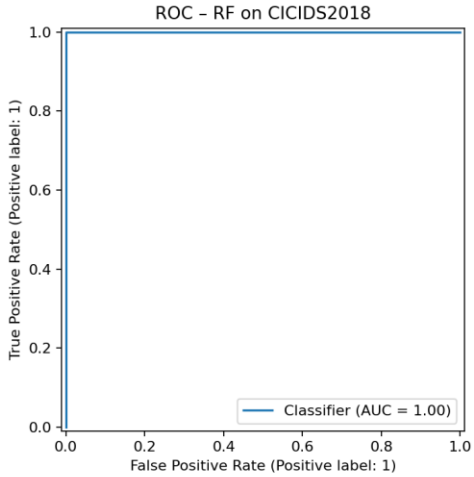

Figure 2: ROC Curve (Random Forest on CICIDS 2018)

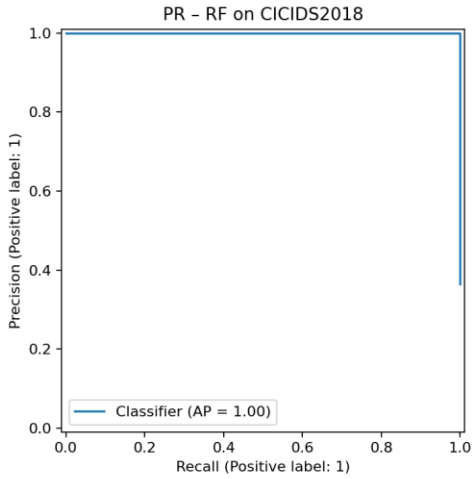

Figure 3: Precision-Recall Curve (Random Forest on CICIDS 2018)

D. Cross-Dataset Generalization

The experiment aimed to determine how machine learning systems would perform in real-world situations:

- Train on CICIDS + ISCX → Test on CTU-1
- Train on CICIDS + CTU-13 → Test on ISCX
- Train on ISCX + CTU-13 → Test on CICIDS

Results showed:

- CICIDS-trained models generalized poorly to CTU-13 (F1 < 0.5), confirming that traffic domain differences and imbalance hinder portability.
- Cross-trained Random Forests achieved moderate recall on ISCX, suggesting some transferable flow-level statistical patterns [11].

E. Feature Importance

The permutation importance factors with top ranks were found to be:

- Flow Duration
- Tot Fwd Pkts / Tot Bwd Pkts
- Flow Pkts/s
- Flow Bytes/s
- Bwd Pkt Len Mean

These properties are causally and temporarily related to dynamic flow intensity and dynamic flow asymmetry, which are key dimensions for exfiltration, scanning, and DoS attack detection.

This demonstrates that the feature of flow has universality, and when applied to anomaly detection techniques, it yields better results [12].

F. Confusion Matrix Insights

Analysis of confusion matrices has shown:

- CICIDS models achieved zero false positives and negatives.
- CTU-13 showed higher false negatives (missed botnets) due to imbalance and subtle malicious flows.

ETA demonstrates outstanding performance in personalization learning within the domain but exhibits poor domain generalization capability, highlighting the need for a federated approach with domain adaptation to detect different EEG signal domains [13].

VII. DISCUSSION

The findings clearly demonstrate that ML models relying on metadata can effectively detect encrypted threats without evaluating payload data. However, outstanding scores on CICIDS 2018 should not be so surprising, as the dataset used for this benchmark is likely much cleaner than live traffic.

A. Insights

- Model Dependence: Ensemble classifiers (RF, GB) outperform linear models when faced with noisy and nonlinear abundance patterns.
- Dataset Bias: Synthetic datasets (CICIDS) yield inflated metrics, while real-world ones (CTU-13) expose limitations.
- Feature Stability: Duration- and rate-based features generalize across datasets; packet-level features are more dataset-specific.
- Operational Trade-off: Higher accuracy often correlates with reduced explainability, emphasizing the need for XAI integration [13].

B. Comparative Context

Framework	Method	Decryption Required	Privacy Risk	Accuracy (avg.)
Traditional IDS (Snort, Suricata)	Payload Signature Matching	✔	High	85–95% (unencrypted only)
Cisco ETA	Flow + TLS Fingerprints	✘	Low	~96%
Proposed ML ETA	Flow Metadata + ML	✘	Low	92–99% (CICIDS)

This discovery seems to coincide remarkably with the Future Industrial Encryption Traffic Analytics (ETA) predictive behaviors and platform manufacturers' trend in (Cisco, Palo Alto, Cortex, XDR, etc.,) following the model anomalies using generic flow streams and machine learning rather than requiring packet-level content [14].

VIII. CONCLUSION AND FUTURE SCOPE

A. Summary of Findings

The search provides proof that Machine learning based Encrypted Traffic Analytics (ETA) can spot malicious encrypted flows precisely, without having to decrypt. Across three diverse datasets:

- CICIDS 2018 achieved near-perfect classification due to high-quality feature separation.
- CTU-13 Botnet presented real-world difficulty with partial success (F1 ≈ 0.55).
- ISCX VPN-nonVPN contributed insight into VPN traffic representation, though limited by single-class subsets.

B. Key takeaways:

- Highly detailed metadata may be generated, but these more detailed features do not seem to be necessary to obtain high classification accuracy.
- Building fewer, more global features seems to work just as well as many more local features.
- Generalizing models to data from multiple, disparate domains remains an open problem.
- Privacy-preserving data analytics, through the capability of selectively sharing features rather than real-valued data, appears to be a practical next step for real-world data science [14].

C. Limitations

- Dataset imbalance and synthetic labelling limit real-world representativeness.
- Lack of QUIC and modern TLS 1.3 traffic reduces contemporary relevance.
- Absence of deep explainability (e.g., SHAP values) constrains interpretability.

D. Future Directions

- Decentralized AI for Security: Develop techniques using decentralized AI for processing sensor data. For instance, consider developing AI algorithms that leverage decentralized computation approaches, such as federated learning [15].
- Adversarial Robustness: Furthermore, create models that improve sensor signal processing (SNAP) to process data either at the data source or at the federated data repository, thereby preventing the need for centralized coordination of more compute-intensive algorithms that run at the data source to improve information security and privacy.
- Explainable AI: Integrate approaches to ensure the trust of users who are affected by the decisions made by AI systems.
- Adversarial ML: Develop and employ approaches and incentives to prevent the subversion of AI as a technology and as developed systems. Where potential adversarial or other misuse scenarios are identified, develop mechanisms to ensure that achieving large-scale harm or impact is sufficiently complex [15].
- Machine Learning Knowledge Creation: Create better mechanisms for ensuring data quality by focusing on the imposition of rules.

REFERENCES:

[1]. Akpaku, E., Chen, J., Ahmed, M., Leslie Brown-Acquaye, W., Kwadzo Agbenyegah, F., & Nii Ayitey Sosu, R. (2025). Detecting encrypted malicious traffic with HEAT: a header-focused deep learning approach. The Computer Journal, bxaf093.

[2]. Alwhbi, I. A., Zou, C. C., & Alharbi, R. N. (2024). Encrypted network traffic analysis and classification utilizing machine learning. Sensors, 24(11), 3509.

[3]. Bakhshi, T., & Ghita, B. (2021). Anomaly detection in encrypted internet traffic using hybrid deep learning. Security and Communication Networks, 2021(1), 5363750.

[4]. Cherukuri, A. K., Ikram, S. T., Li, G., & Liu, X. (2024). Encrypted Network Traffic Analysis. In Encrypted Network Traffic Analysis (pp. 19-45). Cham: Springer International Publishing.

[5]. Fu, Z., Liu, M., Qin, Y., Zhang, J., Zou, Y., Yin, Q., ... & Duan, H. (2022, October). Encrypted malware traffic detection via graph-based network analysis. In Proceedings of the 25th International Symposium on Research in Attacks, Intrusions and Defenses (pp. 495-509).

[6]. Hendaoui, F., Ferchichi, A., Trabelsi, L., Meddeb, R., Ahmed, R., & Khelifi, M. K. (2024). Advances in deep learning intrusion detection over encrypted data with privacy preservation: a systematic review. Cluster Computing, 27(7), 8683-8724.

[7]. Ji, I. H., Lee, J. H., Kang, M. J., Park, W. J., Jeon, S. H., & Seo, J. T. (2024). Artificial intelligence-based anomaly detection technology over encrypted traffic: A systematic literature review. Sensors, 24(3), 898.

[8]. Lupari, P. (2021). Detecting Anomalies in TLS Traffic Using Encrypted Traffic Analysis.

[9]. Papadogiannaki, E., & Ioannidis, S. (2021). Acceleration of intrusion detection in encrypted network traffic using heterogeneous hardware. Sensors, 21(4), 1140.

[10]. Papadogiannaki, E., Tsirantonakis, G., & Ioannidis, S. (2022, June). Network intrusion detection in encrypted traffic. In 2022 IEEE Conference on Dependable and Secure Computing (DSC) (pp. 1-8). IEEE.

[11]. Sharma, A. (2025). XAI-Driven Malicious Encrypted Traffic Detection and Characterization to Enhance Information Security.

[12]. Shen, M., Ye, K., Liu, X., Zhu, L., Kang, J., Yu, S., ... & Xu, K. (2022). Machine learning-powered encrypted network traffic analysis: A comprehensive survey. IEEE Communications Surveys & Tutorials, 25(1), 791-824.
[13]. Uğurlu, M., Doğru, İ. A., & Arslan, R. S. (2021). A new classification method for encrypted internet traffic using machine learning. Turkish Journal of Electrical Engineering and Computer Sciences, 29(5), 2450-2468.
[14]. Wei, L., Wang, Y., Li, X., Li, J., Huang, Y., & Liu, Z. (2025). A Detection Method for Malware Communication Traffic via Encrypted Traffic Analysis. IEEE Internet of Things Journal.
[15]. Yang, L., Fu, S., Wang, Y., Liang, K., Mo, F., & Liu, B. (2023). DEV-ETA: An interpretable detection framework for encrypted malicious traffic. The Computer Journal, 66(5), 1213-1227.