Islamic University of Gaza
Faculty of Information Technology
Department of Graduate Studies
Information Technology Specialization

الجامعـــــة الإســـلاميـة بغـزة
كليـة تكنـولـوجيـا المعلـومـات
قـســم الـدراســات العلـيـا
تخصص تكنولـوجيـا المعلومـات

Report:

AI-Powered Threat Detection through Encrypted Network Traffic Analysis

Cyber security Course

Prepared by:

Alaa Emad Al Hoot **120233046**

Submitted to:

Dr. Tawfiq Barhoum

December 01, 2025

Table of Contents

1.Abstract:

AI is used today to analyze encrypted network traffic without breaking the encryption. Most attacks occur within encrypted channels like HTTPS and TLS, making them difficult for traditional methods to detect. The research relies on analyzing data such as packet size, timing, and the number of streams, rather than the content itself. We test several algorithms, including Random Forest, XGBoost, CNN, and LSTM, to achieve fast and accurate detection. We use data from datasets like CIC-IDS2018 to train the models. The work focuses on maintaining privacy by analyzing only metadata. The goal is to build an intelligent system that detects attacks within encrypted traffic in real time without compromising privacy.

2.Introduction:

There is a serious challenge in contemporary network security: that encrypted traffic currently represents over 95% of all web communications [1]. While cryptographic protocols such as TLS 1.3, HTTPS and QUIC do provide protection of user privacy, they also make it harder to inspect malicious activity by legacy security infrastructure. Machine learning has become an effective tool to extract informative features from encrypted traffic, without the access of payload contents[2], for threat identification while still ensuring user privacy [3].

Cybercriminals increasingly exploit encrypted channels for malware distribution, command-and-control communications, and data exfiltration [4]. Traditional Deep Packet Inspection (DPI) becomes ineffective when payloads are encrypted, creating significant security blind spots. This research addresses the fundamental question: how can we detect malicious behavior within encrypted network flows without compromising encryption itself?

3.Research Objectives:

The goal of this study is to create a smart, secure approach toward detecting potential threats in network (local/remote) propagation using an integrated platform that provides:

1) a means of extracting meaningful patterns from encrypted traffic data
2) a systematic evaluation of machine-learning capabilities to provide an accurate assessment of potential threats to networks
3) the ability to provide real-time alerts for enterprises where user privacy is protected in accordance with relevant privacy legislation.

4. Challenges in Encrypted Traffic Inspection:

Encrypted Traffic Analysis poses numerous significant challenges that are not present with conventional Network Security measures:

- Limited Visibility - Since there is no visibility into the payloads of encrypted messages as they traverse the network through an encrypted communication channel, Security systems must utilize metadata only; this includes packet sizes, timestamps, flow durations, and distributions of packets statistically [5], requiring Security systems to utilize limited Feature spaces in order to build Threat signatures.
- Class Imbalance - Most Network Traffic datasets contain a large imbalance between the Classes, typically with Malicious Traffic accounting for less than 5% of total Network Flow Records [6], leading to ML-based systems with an inherent bias toward the Majority Class and less sensitivity for Rare yet Critical Attacks.
- Concept Drift - The Network behavior is constantly changing, as Applications are Updated, Protocols are modified, as well as Attackers changing their Techniques [7]. Therefore, the ML models must maintain accuracy despite changes in Time, which necessitates Models have the ability to Continually Learn and Adapt.
- Adversarial Evasion - Sophisticated Attackers will deploy techniques designed to evade detection such as obfuscation of network traffic through Timing manipulations, mimicry of benign Applications using Traffic Obfuscation, and so forth [8]; hence, the ML models must be able to withstand these types of Adversarial Evasion techniques while maintaining low levels of False Positive rates.
- Real-time Processing Requirement - The Enormous Volume of Traffic generated by Enterprise Networks necessitates that Analyzing this Traffic be performed at Maximum Speed (line rate); thus, the ML Models must balance Detection Accuracy with Computational Efficiency to allow for Deployment in High-Throughput Environments without introducing intolerable Latencies.
-

5. ML-Based Detection Approaches

According to recent studies on both conventional machine Learning and Deep learning architectures to analyses encrypted data, the latest Developments appear to offer hopeful outcomes.

5.1 Conventional Machine Learning :

About Encryption-based attacks, some researchers have experimented with various conventional ML methods such as Support Vector Machines (SVM), Convolutional Neural Networks (CNN),[9] Random Forests and extreme Gradient Boosting (XGBoost) combined with engineered characteristics based upon Packet Length Distribution, Flow Statistics and Inter-arrival Times (IAT); thus, producing acceptable accuracy levels (<5% FP Rate).

The advantages of using these models include their interpretability,[10] effective training process, and ability to perform real-time inference operations (<1 MS for each Flow), which allows these models to be ideal candidates for analysis in environments with increased amounts of traffic.

5.2Deep Learning Architecture :

- Convolutional Neural Networks (CNNs): 1D-CNNs process packet sequences to detect local patterns in encrypted flows, achieving 94-96% accuracy without manual feature engineering [11]. Multiple convolutional layers extract hierarchical representations from raw traffic data.
- Recurrent Neural Networks (LSTMs): Bidirectional LSTMs capture temporal dependencies across network sessions, proving particularly effective for session-based attacks and advanced persistent threats. These models excel at modeling sequential behavior patterns that traditional methods miss [12].
- Hybrid Architectures: Combining CNN for spatial feature extraction with LSTM for temporal modeling leverages complementary strengths, achieving 97-98% detection accuracy [13]. Attention mechanisms further enhance performance by identifying which packets contribute most to classification decisions, improving both accuracy and interpretability.

5.3 Emerging Approaches

Graph Neural Networks model network communication as graphs where nodes represent endpoints and edges represent flows, capturing relational patterns invisible to traditional methods [14]. Self-supervised learning approaches reduce dependency on labeled data, addressing the scarcity of annotated attack traffic [15].

6. Datasets for Encrypted Traffic Analysis:

The high-quality dataset is an important part of developing and testing machine learning models. There are multiple benchmark datasets that will allow you to do research into encrypted traffic.

- CIC-IDS2018: This dataset contains seven attack scenarios - Brute-force, Heartbleed, Botnet, DoS, DDoS, Web attack, and Infiltration – with 50 attacking computers attacking an organization that has 420 PCs and 30 servers [16][17]. There are around 16 million labelled flows, with 80 pre-extracted features, that simulate the latest behavior and protocols of a network and also the newest encryption technologies.

- CICIDS2017: This earlier dataset consists of many types of diverse attacks (SSH brute force, Infiltration, and Botnet traffic), and while some of the attacks included in the dataset have already been captured in the past, this dataset is often used for benchmarking due to the realistic traffic patterns contained in it [18].

- USTC-TK2016: This dataset focuses solely on malware traffic, and it provides flows of 10 different malware families that communicate using TLS-encrypted connections. This dataset has the ability to evaluate a malware-specific detection capability [19].

- CTU-13: The CTU-13 dataset contains captured network traffic from a total of 13 different botnet scenarios, and it also concentrates on command-and-control traffic captured and transmitted via encrypted channels [20]. The CTU-13 dataset will also help determine how well an organization can identify stealthy long-term intrusions.

Each of the above datasets has its own unique characteristics, in terms of the type of protocols that they cover, the different types of attacks that occur, and their temporal relevancy. As a result, researchers need to match the datasets that they intend to use in their studies to the specific goals of their studies and also to understand the limitations on generalization when evaluating machine learning models that were trained and tested on network traffic captured in the past or using artificial datasets.

7. Privacy and Ethical Considerations:

The deployment of ML-based encrypted traffic analysis raises significant privacy and ethical concerns that must be carefully addressed to ensure responsible implementation.

7.1 Designing for Privacy

Our approach for designing solutions adheres to the Principles of Privacy by Design by processing only metadata information (not payloads)[21]. The features are intentionally designed not to allow for the identification of a user based on an analysis of flow-level statistics (as opposed to packet-level analysis). Our model training processes will use the technique of Differential Privacy; whereby calibrated noise is added during model training so that specific traffic pattern memorization will not occur. As such, the model parameters cannot be used to reconstruct individual flows [22].

7.2 Ethical Considerations

Surveillance Potential: Network monitoring may lead to potential surveillance if used inappropriately. Therefore, organizations should implement robust policies regarding the types of analysis that can be performed, as well as appropriate oversight mechanisms for when network traffic analysis may occur [23].

Algorithmic Bias: The training dataset may not be a fair representation of the full user population and could therefore create discriminatory outcomes in identifiable areas and applications. To ensure fairness among users, organizations must conduct regular audits of model fairness and ensure diversity within training datasets [24].

Transparency and Accountability: Users should be made aware that traffic analysis is being conducted, and organizations should provide the ability for users to understand why certain detections were made. The use of attention-based models increases transparency by indicating the types of signal characteristics that led to an alert [25].

7.3 Legal Compliance

GDPR allows for the use of traffic analysis for the legitimate security purposes of organizations, while still requiring organizations to balance the privacy rights of their users[26] . Our methodology does not decrypt payloads and does not store user traffic data, therefore allowing for regulatory compliance under all of the major regulatory frameworks, including HIPAA, FISMA, PCI-DSS, etc.

8. Conclusion:

The ability of an AI-based approach to detect threats hidden within encrypted traffic illustrates not only technical feasibility but also ethical viability, provided that privacy is at the core of the design's foundation. Using existing data only (via metadata features), machine-learning techniques, specifically CNN + LSTM hybrids, have shown 97% - 98% accuracy in threat detection where encryption exists, indicating that encryption does not have to be compromised for effective security.

That said, remaining challenges include further study into adversarial robustness related to complex evasion techniques; adaptation to the continual changes of temporal distributions and behaviors present in networks as they change and grow; and the need to broaden both operational and incorporation of emerging protocols (QUIC, DNS-over-HTTPS) from legacy protocols. Most importantly, the continued lack of explanation about how these detection methods work has limited the level of trust or debugging abilities available.

To this end, furthering current research should include exploring federated learning for privacy-preserving cooperative activities between multiple organizations, opportunities to incorporate existing threat intelligence into newly developed methods for context-based detection, and expanding capabilities to handle encrypted IoT traffic with the same or differing characteristics as other encrypted forms. As threats continue to evolve, AI will become increasingly necessary—provided data privacy remains a primary consideration in all advancements in technology.

Moving forward will require creating regulatory governance structures, being transparent with stakeholders, performing ongoing auditing related to potential biases, and strictly limiting the collection of customer data.—In short, future organizations adopting proactive security measures should ensure they are mindful of their users' privacy—this will help establish a level of trust between the user and the organization while providing users with greater assurance that their privacy cannot be compromised due to technological advancements.

9. References:

[1] M. Shen *et al.*, “Machine Learning-Powered Encrypted Network Traffic Analysis: A Comprehensive Survey,” *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 791–824, Nov. 2023, doi: 10.1109/COMST.2022.3208196.

[2] I. A. Alwhbi, C. C. Zou, and R. N. Alharbi, “Encrypted Network Traffic Analysis and Classification Utilizing Machine Learning.,” *Sensors (Basel)*, vol. 24, no. 11, May 2024, doi: 10.3390/s24113509.

[3] M. J. de Lucia and C. Cotton, “Detection of Encrypted Malicious Network Traffic using Machine Learning,” in *MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM)*, IEEE, Nov. 2019, pp. 1–6. doi: 10.1109/MILCOM47813.2019.9020856.

[4] V. A. Muliukha, L. U. Laboshin, A. A. Lukashin, and N. V. Nashivochnikov, “Analysis and Classification of Encrypted Network Traffic Using Machine Learning,” in *2020 XXIII International Conference on Soft Computing and Measurements (SCM)*, IEEE, May 2020, pp. 194–197. doi: 10.1109/SCM50615.2020.9198811.

[5] I. A. Alwhbi, C. C. Zou, and R. N. Alharbi, “Encrypted Network Traffic Analysis and Classification Utilizing Machine Learning,” *Sensors*, vol. 24, no. 11, p. 3509, May 2024, doi: 10.3390/s24113509.

[6] Y. Zeng, P. Chen, and J. Zhang, “Monitoring and Analysis of Encrypted Attack Traffic Based on Machine Learning,” in *2023 International Conference on Human-Centered Cognitive Systems (HCCS)*, IEEE, Dec. 2023, pp. 1–9. doi: 10.1109/HCCS59561.2023.10452583.

[7] F. Bragone, K. Oueslati, T. Laneryd, M. Luvisotto, and K. Morozovska, “Physics-Informed Neural Networks for Modeling Cellulose Degradation in Power Transformers,” in *2022 21st IEEE International Conference on Machine Learning and Applications (ICMLA)*, IEEE, Dec. 2022, pp. 1365–1372. doi: 10.1109/ICMLA55696.2022.00216.

[8] S. Jorgensen *et al.*, “Extensible Machine Learning for Encrypted Network Traffic Application Labeling via Uncertainty Quantification,” *IEEE Transactions on Artificial Intelligence*, vol. 5, no. 1, pp. 420–433, Jan. 2024, doi: 10.1109/TAI.2023.3244168.

[9] Z. Wang, K. W. Fok, and V. L. L. Thing, “Machine learning for encrypted malicious traffic detection: Approaches, datasets and comparative study,” *Comput Secur*, vol. 113, p. 102542, Feb. 2022, doi: 10.1016/j.cose.2021.102542.

[10] T. Chen and C. Guestrin, “XGBoost,” in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, New York, NY, USA: ACM, Aug. 2016, pp. 785–794. doi: 10.1145/2939672.2939785.

[11] Z. Zhu, H. Zhou, Q. Yang, C. Wang, and Z. Li, “Anomaly Detection in Encrypted Identity Resolution Traffic based on Machine Learning,” in *2022 IEEE 22nd International Conference on Software Quality, Reliability and Security (QRS)*, IEEE, Dec. 2022, pp. 264–275. doi: 10.1109/QRS57517.2022.00036.

[12] G. Baldini, “Analysis of Encrypted Traffic with time-based features and time frequency analysis,” in *2020 Global Internet of Things Summit (GIoTS)*, IEEE, Jun. 2020, pp. 1–5. doi: 10.1109/GIOTS49054.2020.9119528.

[13] V. Kanimozhi and T. P. Jacob, “Artificial Intelligence based Network Intrusion Detection with Hyper-Parameter Optimization Tuning on the Realistic Cyber Dataset CSE-CIC-IDS2018 using Cloud Computing,” in *2019 International Conference on Communication and Signal Processing (ICCSP)*, IEEE, Apr. 2019, pp. 0033–0036. doi: 10.1109/ICCSP.2019.8698029.
[14] A. Vaswani *et al.*, “Attention Is All You Need,” Aug. 2023.
[15] J. Snoek, H. Larochelle, and R. P. Adams, “Practical Bayesian Optimization of Machine Learning Algorithms,” Aug. 2012.
[16] A. M. Elshewey and A. M. Osman, “Enhancing encrypted HTTPS traffic classification based on stacked deep ensembles models,” *Sci Rep*, vol. 15, no. 1, p. 35230, Oct. 2025, doi: 10.1038/s41598-025-21261-6.
[17] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization,” in *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, SCITEPRESS - Science and Technology Publications, 2018, pp. 108–116. doi: 10.5220/0006639801080116.
[18] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, “SMOTE: Synthetic Minority Over-sampling Technique,” *Journal of Artificial Intelligence Research*, vol. 16, pp. 321–357, Jun. 2002, doi: 10.1613/jair.953.
[19] H.-H. Huynh, X.-H. Nguyen, X.-D. Nguyen, and K.-H. Le, “Bigsids: an efficient SDN-based network intrusion detection systems for big data environments,” *Cluster Comput*, vol. 28, no. 6, p. 395, Sep. 2025, doi: 10.1007/s10586-024-05075-1.
[20] K. Ibrahimi, M. Jouhari, and Z. Jakout, “Enhancing Intrusion Detection Systems Using Machine Learning Classifiers on the CSE-CIC-IDS2018 Dataset,” in *2024 11th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, IEEE, Jul. 2024, pp. 1–6. doi: 10.1109/WINCOM62286.2024.10655131.
[21] A. Cavoukian, “Privacy by Design: The 7 Foundational Principles (Longer Version)(https://student.cs.uwaterloo.ca/~cs492/papers/7foundationalprinciples_longer.pdf),” Waterloo, Oct. 2011.
[22] M. Abadi *et al.*, “Deep Learning with Differential Privacy,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA: ACM, Oct. 2016, pp. 308–318. doi: 10.1145/2976749.2978318.
[23] M. Brundage *et al.*, “The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation,” Dec. 2024.
[24] C. Rudin, “Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead,” *Nat Mach Intell*, vol. 1, no. 5, pp. 206–215, May 2019, doi: 10.1038/s42256-019-0048-x.
[25] L. Göcs and Z. C. Johanyák, “Identifying relevant features of CSE-CIC-IDS2018 dataset for the development of an intrusion detection system,” *Intelligent Data Analysis*, vol. 28, no. 6, pp. 1527–1553, Nov. 2024, doi: 10.3233/IDA-230264.
[26] C. of the E. U. European Parliament, “General Data Protection Regulation (GDPR)(https://eur-lex.europa.eu/eli/reg/2016/679/oj),” Brussels, Apr. 2016.