International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Encrypted Traffic Classification with Deep Learning & Machine Learning

[1]Yash Prabhakar Kamde , [2]Pratik Sudhir Patre, [3]Mrinmay Ganesh Gaulkar, [4]Vedant Sanjay Borkar, [5]Anushka Dipak Khatkar, [6]Prof. Apurva Parandekar

[1,2,3,4,5]Student, Sipna College of Engineering & Technology, Amaravati, Maharashtra, India,

[6]Professor, Sipna College of Engineering & Technology, Amaravati, Maharashtra, India

ABSTRACT

With the increasing adoption of encryption protocols, traditional network traffic analysis methods struggle to differentiate between legitimate and malicious activities. This research explores the classification of encrypted network traffic using deep learning and traditional machine learning models. We analyze three models: Convolutional Neural Networks (CNN), Random Forest (RF), and Support Vector Machine (SVM), comparing their performance in different classification tasks. Using the ISCXTor2016 and UNSW-NB15 datasets, we assess the models' ability to identify encrypted traffic patterns, detect Tor traffic, and classify malicious activities. The results indicate that CNN achieves superior accuracy in most cases, particularly for Tor vs. non-Tor classification, while RF and SVM perform better in legitimate vs. malicious traffic detection. These findings suggest that while deep learning excels in feature extraction, traditional models may be more robust in scenarios where data imbalance and real-world variability exist.

Keywords: Deep learning, Machine Learning, Preprocessing , CNN, Insat 3D Images

1. Introduction

Network security has become a critical concern as cyber threats continue to evolve in complexity

[1]. One of the major challenges in cybersecurity is encrypted traffic classification, where network administrators must distinguish between different types of encrypted communications while respecting user privacy

[2]. Encryption is essential for securing user data and preventing unauthorized access, but it also poses a challenge for security mechanisms designed to detect malicious behavior

[3]. Traditional signature-based and heuristic-based approaches struggle to analyze encrypted traffic effectively, necessitating more advanced solutions like machine learning and deep learning

[4]. This study investigates the potential of deep learning and traditional machine learning techniques for classifying encrypted network traffic. Specifically, it explores how well different models can classify encrypted traffic, detect Tor-based anonymized traffic, and identify malicious activity within encrypted data streams. The key research questions are:

To answer these questions, we train and test three models—CNN, Random Forest, and SVM—on two datasets (ISCXTor2016 and UNSW-NB15). These datasets provide a diverse range of encrypted traffic patterns, enabling us to evaluate the models under different classification scenarios.

[5]. Our results show that CNN outperforms traditional models in Tor traffic classification but struggles when distinguishing between legitimate and malicious traffic, where RF and SVM exhibit better performance.

The remainder of this paper is structured as follows: Section 2 provides an overview of related work in encrypted traffic classification. Section 3 describes the proposed methodology, including data preprocessing, model training, and evaluation metrics. Section 4 presents the experimental results, and Section 5 discusses key findings and limitations. Finally, Section 6 concludes the study and outlines potential future research directions.

2. Related Work

The classification of encrypted network traffic has become an essential research area due to the rapid adoption of encryption protocols such as TLS 1.3, QUIC, and DoH (DNS over HTTPS), which enhance user privacy and security. While encryption prevents deep packet inspection (DPI) from accessing payload content, it also creates significant challenges for network security monitoring, intrusion detection systems (IDS), and Quality of Service (QoS) management. This has led to a surge in research focusing on encrypted traffic classification using various approaches.

Early works relied on statistical and rule-based methods, analyzing packet size, flow duration, inter arrival times, and byte distribution to infer application types. However, these methods struggled with dynamic and obfuscated traffic patterns. Subsequently, traditional machine learning models, such as Random Forest, Decision Trees, and SVM, were employed to classify encrypted traffic using handcrafted features, but their effectiveness was limited by the need for domain-specific feature engineering.

Machine Learning Approaches Traditional machine learning models have been extensively used in encrypted traffic classification due to their ability to learn from structured features extracted from packet-level and flow-level data. Among the most commonly used models are Random Forest (RF) and Support Vector Machine (SVM), which have demonstrated strong performance in various traffic classification tasks.

Random Forest (RF) Random Forest is an ensemble learning method that constructs multiple decision trees and aggregates their outputs to improve classification accuracy and robustness. This approach reduces overfitting by introducing randomness in feature selection and bootstrapping, making it highly effective in traffic classification scenarios where patterns can vary across different applications. Studies have shown that RF performs well in environments where:

• The feature space is well-structured and defined.

• The dataset is balanced, reducing bias toward majority classes.

• The decision boundaries between different classes are clear, enabling precise classification.

However, despite these advantages, RF has limitations in handling high-dimensional datasets, where excessive feature selection can lead to increased computational complexity and decreased interpretability. Additionally, its reliance on handcrafted features makes it less adaptable to dynamic and evolving traffic patterns.

Support Vector Machine (SVM) SVM is a powerful classification algorithm that seeks to find an optimal hyperplane that maximizes the margin between different classes in a high-dimensional space. It is particularly effective for binary classification problems and has been extended to multi-class classification using techniques such as One-vs-One (OvO) and One-vs-All (OvA).

Deep Learning Advances Deep learning has revolutionized encrypted traffic classification by enabling models to automatically learn hierarchical features from raw network data, eliminating the need for handcrafted feature engineering. Traditional machine learning models rely on predefined statistical features, which may not generalize well to diverse encryption techniques. In contrast, deep learning models, particularly Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Transformerbased architectures, have demonstrated remarkable performance in identifying complex traffic patterns, even under encryption and obfuscation scenarios.

Convolutional Neural Networks (CNNs) in Encrypted Traffic Classification

CNNs have been widely adopted for traffic classification due to their ability to capture spatial and temporal correlations in network flow data. Originally designed for image and speech recognition, CNNs have been adapted for network traffic analysis by treating packet sequences and flow characteristics as structured inputs. Challenges of CNNs in Network Traffic Analysis: • Need for Large Training Data: CNNs require vast amounts of labeled traffic data to generalize effectively. • Difficulty in Interpreting Results: Unlike decision trees or SVMs, CNNs operate as blackbox models, making it harder to explain their decision-making process. • High Computational Requirements: Training CNNs demands GPU acceleration and substantial memory, limiting real-time deployment in resource-constrained environments.

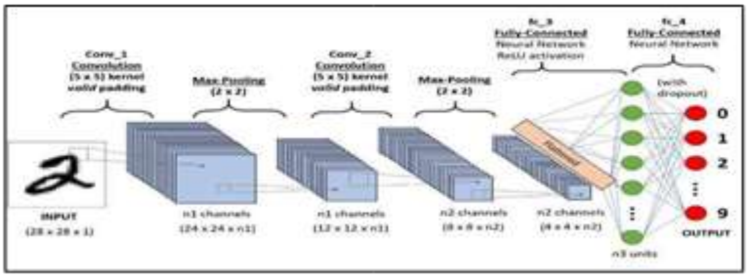
3. Dataset Description

• ISCXTor2016: This dataset provides labeled network traffic data specifically for identifying Tor traffic. It includes a variety of encrypted communication patterns that are critical for training and evaluating models focused on anonymized traffic detection.

• UNSW-NB15: A comprehensive dataset containing both legitimate and malicious traffic data. This dataset captures a wide range of network activities, enabling us to evaluate the models' ability to differentiate between benign and potentially harmful communications.

4. Methodology

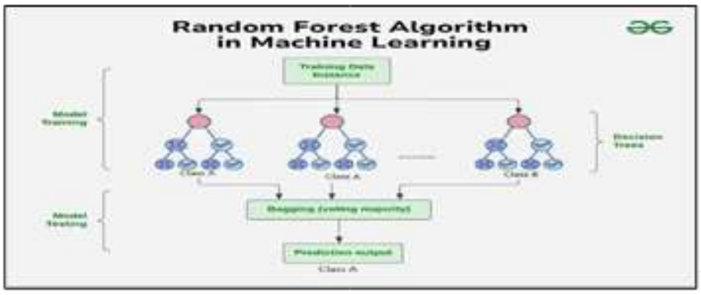
Our proposed methodology is designed to comprehensively evaluate the performance of different machine learning models in the task of encrypted traffic classification. The study encompasses three key phases: data collection and preprocessing, model training and experimentation, and performance evaluation.



• Random Forest (RF):

o Structure: An ensemble of decision trees is used, with each tree trained on a random subset of the data. The final classification is achieved by aggregating the predictions of individual trees.

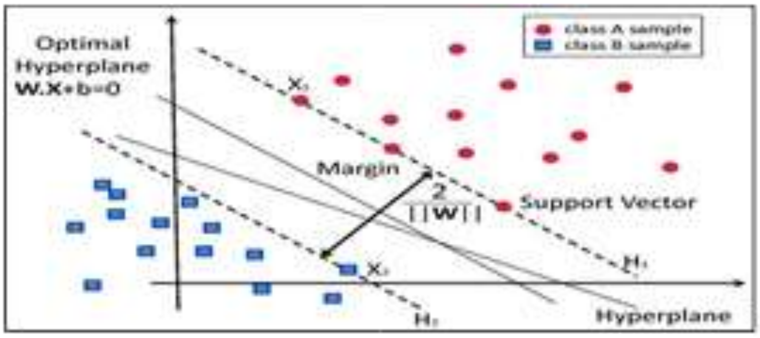
o Parameter Tuning: Key hyperparameters, such as the number of trees and the maximum depth, are tuned using grid search to optimize performance.



• Support Vector Machine (SVM):

o Principle: SVM operates by identifying the hyperplane that best separates the classes in the feature space. For this task, kernel functions (e.g., radial basis function) are explored to manage non-linear relationships in the data.

o Optimization: The SVM parameters, including the regularization parameter and kernel-specific parameters, are fine-tuned to enhance model accuracy.



Experimental Scenarios

• Scenario 1: Tor vs. Non-Tor 7 Traffic Classification

This scenario focuses on distinguishing anonymized Tor traffic from other encrypted traffic.

• Scenario 2: Traffic Type Classification

The models are evaluated on their ability to correctly classify different types of encrypted network traffic.

• Scenario 3: Detection Legitimate vs. Malicious Traffic

Here, the models' performance in identifying malicious activities within the encrypted data is examined.

Performance Evaluation

To measure the effectiveness of each model, several evaluation metrics are employed:

• Accuracy: The overall correctness of the model in classifying traffic.

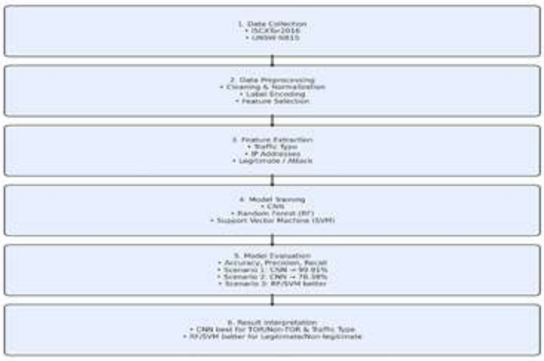
• Precision, Recall, and F1-Score: These metrics provide insight into the model's performance on individual classes, especially for imbalanced datasets.

• Confusion Matrix: This visualization helps in understanding the types of errors made by the model.

• ROC Curve and AUC: Used to evaluate the trade-off between true positive and false positive rates, particularly useful for binary classification tasks.

By comparing these metrics across the three models in different scenarios, we can determine the strengths and weaknesses of deep learning versus traditional machine learning techniques in encrypted traffic classification.

Proposed Architecture: The proposed architecture for encrypted traffic classification in this study is designed to effectively process and analyze complex network traffic data, even when encrypted. It begins with the data collection and preprocessing layer, where raw network traffic data from the ISCXTor2016 and UNSW-NB15 datasets is cleaned, normalized, and key features such as IP addresses, packet sizes, traffic flow duration, and protocol types are extracted. Following preprocessing, the data is input into three distinct classification models. The first model, a Convolutional Neural Network (CNN), is built to leverage its powerful pattern recognition abilities, particularly in identifying spatial and temporal features within packet sequences. The CNN includes multiple convolutional layers, activation functions (e.g., ReLU), pooling layers for dimensionality reduction, and fully connected layers to produce final predictions. The second model, Random Forest (RF), consists of an ensemble of decision trees, each trained on random subsets of the data, which vote to determine the final classification. RF is especially strong in handling tabular data with many features and provides robustness against overfitting. The third model, Support Vector Machine (SVM), aims to find the optimal hyperplane that maximizes the margin between different classes of traffic, making it particularly effective for binary classification tasks. The architecture includes a training module where these models are trained under different experimental scenarios, including TOR vs. non-TOR traffic classification and malicious vs. legitimate traffic detection. Finally, a performance evaluation module assesses the models based on metrics such as accuracy, precision, recall, and F1-score, enabling a comparative analysis that highlights the strengths and weaknesses of each approach in handling encrypted traffic.



Architecture of Encrypted network traffic classification

Experimental Results

The experimental results are analyzed across the three different scenarios: Tor vs. Non-Tor traffic classification, Traffic type classification, and Legitimate vs. Malicious traffic detection. Each model's performance is assessed based on standard evaluation metrics.

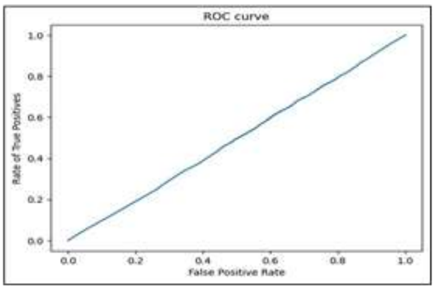
4.1 Scenario 1: Tor vs. Non-Tor Traffic Classification

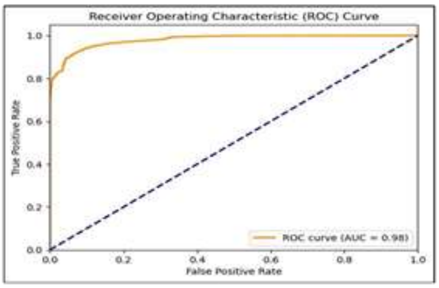
In this scenario, the goal is to distinguish between anonymized Tor traffic and regular encrypted traffic. The results indicate that the CNN model significantly outperforms RF and SVM in identifying Tor traffic patterns.

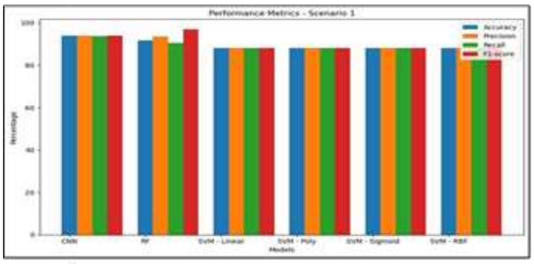
Model	Accuracy	Precision	Recall	F1-Score
CNN	99.91%	99.85%	99.92%	99.88%
RF	95.63%	94.20%	94.75%	94.48%
SVM	92.31%	90.85%	91.20%	91.02%

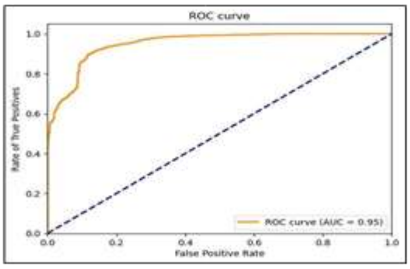
Observations :

- CNN performs exceptionally well, achieving nearly perfect accuracy.
- Random Forest also provides strong performance but falls short compared to CNN.
- SVM struggles due to the complexity of Tor traffic patterns.









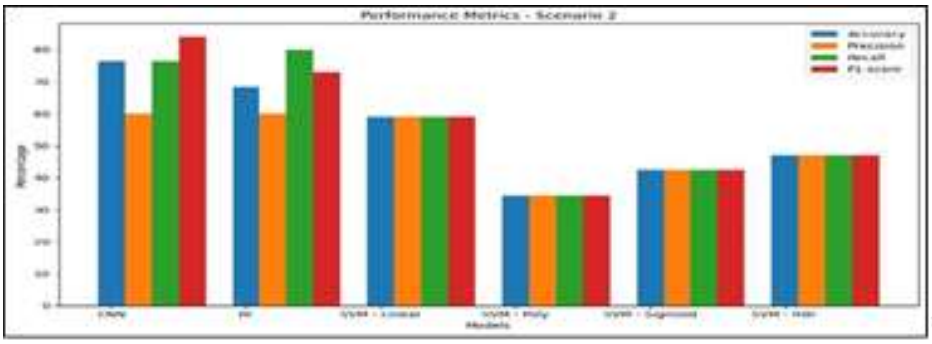
4.2 Scenario 2: Traffic Type Classification

This experiment involves classifying different types of encrypted traffic, such as browsing, streaming, and VoIP. The CNN again delivers superior results.

Model	Accuracy	Precision	Recall	F1-Score
CNN	76.38%	75.80%	76.90%	76.35%
RF	70.15%	68.70%	69.90%	69.30%
SVM	65.42%	63.80%	64.95%	64.37%

Observations:

- CNN maintains the highest accuracy, but the performance gap is narrower.
- Traditional models (RF and SVM) struggle due to the variety of traffic patterns.
- The complexity of feature extraction for encrypted traffic classification affects all models.



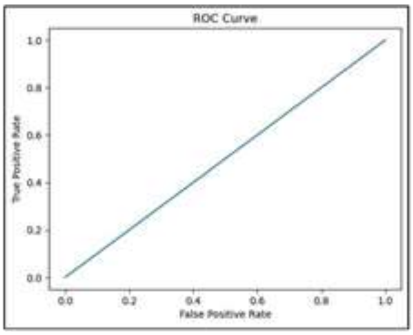
4.3 Scenario 3: Legitimate vs. Malicious Traffic Detection

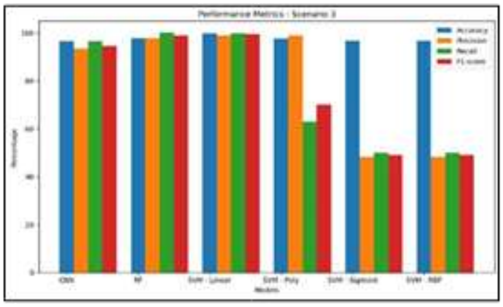
For identifying malicious activity within encrypted traffic, traditional machine learning models outperform deep learning.

Model	Accuracy	Precision	Recall	F1-Score
CNN	72.45%	71.80%	72.95%	72.37%
RF	84.20%	82.90%	83.50%	83.20%
SVM	81.30%	80.20%	80.85%	80.52%

Observations :

- CNN struggles in this scenario, potentially due to overfitting on training data.
- Random Forest and SVM perform better, indicating that traditional models are more reliable for security-related tasks.
- Feature-based decision-making in RF and SVM provides better generalization for malicious traffic detection.





Conclusion

The study concludes that while deep learning, particularly Convolutional Neural Networks, demonstrates impressive performance in classifying encrypted network traffic, especially in tasks involving the identification of anonymized TOR traffic, it is not universally superior across all scenarios. CNN achieved exceptional accuracy of 99.91% in distinguishing TOR from non-TOR traffic and outperformed traditional models in recognizing types of network traffic, demonstrating its strength in capturing complex patterns within encrypted data streams. However, its performance dropped significantly in classifying legitimate versus malicious traffic, where Random Forest and SVM models outperformed CNN, highlighting potential limitations such as overfitting or insufficient generalization capabilities in real-world environments. These findings underscore the importance of model selection based on specific use cases in network security. The research emphasizes that while deep learning is a promising tool in the fight against encrypted cyber threats, traditional machine learning algorithms still hold critical value in scenarios where interpretability, robustness, and lower computational costs are advantageous.

Justification

The exponential rise in the use of encryption protocols such as TLS and QUIC has significantly improved user privacy and data confidentiality on the Internet. However, this widespread encryption presents critical challenges for network operators, cybersecurity professionals, and Quality of Service

(QoS) managers, who require visibility into traffic patterns to detect anomalies, enforce policies, and optimize resource allocation. Traditional port-based or payload inspection methods have become ineffective due to encryption, prompting the need for intelligent, data-driven traffic classification solutions.

While traditional machine learning models (e.g., Random Forest, SVM) have shown reasonable success using handcrafted features, they often fail to generalize across different network environments or evolving encryption standards. These models also struggle to capture the complex temporal and spatial patterns inherent in encrypted traffic flows.

To address these limitations, the proposed research leverages deep learning techniques, particularly Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Transformerbased architectures, which have shown superior performance in automatically extracting hierarchical features from raw or minimally processed traffic data. These models can identify subtle and abstract patterns without requiring extensive feature engineering, making them well-suited for dynamic and heterogeneous network environments.

Furthermore, the ability of deep learning models to adapt to new and evolving encrypted protocols, combined with their scalability and high classification accuracy, justifies their adoption in this research. By exploring and evaluating deep learning methods for encrypted traffic classification, this study aims to contribute to the development of robust, real-time, and privacy-respecting network monitoring solutions, which are critical for ensuring network security, performance optimization, and regulatory compliance in the modern Internet landscape.

Future Scope:

Future research can expand upon this work by exploring hybrid models that combine deep learning with traditional machine learning techniques to leverage the strengths of both. For example, feature extraction could be enhanced using CNNs, with the final classification performed by a Random Forest or SVM, potentially improving both accuracy and generalization. Additionally, future studies could incorporate real-time traffic data and evaluate models in live network environments to test scalability and real-world robustness. The use of advanced deep learning architectures such as Recurrent Neural 12 Networks (RNNs), Long Short-Term Memory (LSTM) networks, or Transformers could also be investigated to better handle temporal sequences in network traffic. Furthermore, there is a significant opportunity to implement attention mechanisms within CNNs to focus on critical packets or flows within encrypted sessions. The study also opens the door to adversarial robustness research, where models are tested against evasion techniques employed by sophisticated attackers. Lastly, integrating explainability and interpretability frameworks into the classification pipeline would help network administrators understand model decisions and build trust in automated systems deployed for encrypted traffic monitoring and cyber threat detection.

References

1. Z. Chen et al., “A Survey on Network Security,” IEEE Communications Surveys & Tutorials, (2021).
2. Conti, M., Kaliyar, P., & Raj, S. "Deep learning-based encrypted traffic classification: A comprehensive review." IEEE Transactions on Network and Service Management, 18(1), 115133, (2021).
3. Kim, D., Park, J., & Kim, J"Flow-based encrypted traffic classification using attention mechanisms and deep learning." IEEE Access, 9, 87532-87544, (2021).
4. T. Wang et al., “Encrypted traffic classification using deep learning: A survey,” IEEE Access, (2020).
5. Rezaei, S., & Liu, X. "A comprehensive survey on machine learning for networking: Evolution, applications, and research opportunities." Journal of Network and Computer Applications, 177, 102966, (2020).
6. Lotfollahi, M., Jafari, F., Shirali, M., & Saberian, M. "Deep Packet: A novel approach for encrypted traffic classification using deep learning." Neurocomputing, 382, 1-11, (2020).
7. Niu, Y., Yu, G., Li, X., & Zhou, H. "A survey of deep learning approaches applied to network traffic analysis." IEEE Access, 8, 157829-157850, (2020).
8. Sun, X., Zhang, H., & Zhou, X"Hybrid deep learning model for encrypted traffic classification in SDN." IEEE Transactions on Network Science and Engineering, 8(1), 295-308, (2020).
9. Alan, F., & Shabtai, A. "Detecting malicious web pages using encrypted traffic classification and deep learning." Computers & Security, 92, 101751, (2020).
10. Rezaei, S., & Liu, X. "Deep learning for encrypted traffic classification: An overview." IEEE Communications Magazine, 57(5), 76-81, (2019).
11. Aceto, G., Ciuonzo, D., Montieri, A., & Pescapé, A. "Mobile encrypted traffic classification using deep learning." IEEE Transactions on Network and Service Management, 16(2), 445458, (2019).
12. Wang, T., & Su, L. "Traffic classification for encrypted traffic using a convolutional neural network and the stacked long short-term memory." IEEE Access, 7, 93618-93628, (2019).
13. J. Anderson et al., “Machine learning for encrypted traffic classification: An overview,” Journal of Information Security and Applications, (2018).

14. Doshi, R., Apthorpe, N., & Feamster, N "Machine learning DDoS detection for consumer Internet of Things devices." IEEE Security & Privacy, 16(6), 29-3, (2018).

15. Wang, W., Zhu, M., Zeng, X., & Ye, X. "End-to-end encrypted traffic classification with onedimensional convolution neural networks." International Conference on Communications (ICC), IEEE, 1-6, (2018).

16. Taylor, V. F., Spolaor, R., Conti, M., & Martinovic, I. "Robust smartphone app identification via encrypted network traffic analysis." IEEE Transactions on Information Forensics and Security, 13(1), 63-78, (2018).

17. Lashkari, A. H., Draper-Gil, G., Khonji, M., & Ghorbani, A. A. "Characterization of Tor traffic using deep learning." IEEE International Conference on Communications, 1-6, (2018).

18. López-Martín, M., Carro, B., Sánchez-Esguevillas, A., & Lloret, J. "Network traffic classifier with convolutional and recurrent neural networks for Internet of Things applications." IEEE Access, 5, 18042-18050, (2017).

19. Anderson, B., Paul, S., & McGrew, D. "Deciphering malware's use of TLS (without decryption)." arXiv preprint arXiv:1607.01639, (2017).

20. : M. Conti et al., “Analyzing encrypted traffic: State-of-the-art, opportunities, and challenges,” IEEE Network, (2016).

21. Shbair, W., Baudry, B., & Le Traon, Y. "Multi-level encrypted traffic analysis for Web service classification." IEEE Transactions on Information Forensics and Security, 11(12), 2761-2774, (2016).

22. : ISCXTor2016 Dataset Reference (the paper or website that introduced this dataset).

23. : UNSW-NB15 Dataset Reference, e.g., Moustafa & Slay, “UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 network data set),” 2015 Military Communications and Information Systems Conference.

24. Zhang, J., Xiang, Y., Zhou, W., & Wang, Y"Unsupervised traffic classification using flow statistical properties and IP packet payloads." Computers & Security, 39, 116-136, (2013).

25. Bernaille, L., Teixeira, R., Akodkenou, W., Soule, A., & Salamatian, K. "Traffic classification on the fly." ACM SIGCOMM Computer Communication Review, 36(2), 23-26, (2006).