International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 06 | June - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

A Survey on Machine Learning Techniques for the Classification of Encrypted Network Traffic

Balashanthi Gopal [1] Dr. J. C. Miraclin Joyce Pamila [2]

[1] Department of CSE, Government College of Technology, Coimbatore, India bala.71772377104@gct.ac.in

[2] Head of The Department CSE, Government College Of Technology, Coimbatore, India miraclin@gct.ac.in

Abstract

Due to encrypted network traffic growth, complex machine learning (ML) algorithms are required to label applications accurately. This is because of problems connected with traditional traffic categorization in encrypted communications, especially with the use of obfuscation techniques such as VPNs. The questionnaire detected several serious issues, such as privacy problems, complexity of calculations, and applicability to unknown traffic. It finds research gaps and possible fixes, for example, combining explainable AI, adversarial learning, and uncertainty quantification to enhance classification interpretability and robustness. This survey deeply studies current machine learning (ML)-based approaches for classifying encrypted communication and evaluating their benefits, drawbacks, and suitability for practical application. This work is based on the research described in Extensible Machine Learning for Encrypted Network Traffic Application Labeling via Uncertainty Quantification.

Keywords: Encrypted Network Traffic, Machine Learning, Virtual Private Networks, Traffic Classification, Uncertainty Quantification, Explainable AI.

I. Introduction

The quick increase in encrypted network traffic has greatly enhanced user security and privacy. But it has also presented substantial challenges for traffic classification, anomaly detection, and network monitoring. Due to encryption algorithms that mask packet content, existing rule-based and signature-based techniques that depend on deep packet inspection (DPI) are no longer viable. Consequently, machine learning (ML) has become a potent substitute for distinguishing encrypted network traffic according to behavioral and statistical characteristics. Using variables that includes packet sizes, inter-arrival durations, and flow-level data, machine learning (ML)-based traffic classification uses supervised, unsupervised, and semi-supervised learning approaches. Although these methods have shown encouraging outcomes, they still have problems, especially when it comes with handling traffic from Virtual Private Networks (VPNs), traffic hiding, and zero-day assaults. Furthermore, the majority of machine learning models are devoid of uncertainty quantification techniques, which are essential for practical implementation. The strengths, drawbacks, and unmet research needs of machine learning techniques employed in encrypted traffic classification are thoroughly addressed in this survey. It builds upon the references cited in the study "Extensible Machine Learning for Encrypted Network Traffic Application Labeling via Uncertainty Quantification" [1]. Furthermore, it identifies open research challenges and explores potential solutions to enhance the effectiveness and reliability of ML models in this domain.

II. Existing Work

1. Encrypted Internet Traffic Classification Using a Supervised Spiking Neural Network

This paper introduces the use of Spiking Neural Networks (SNNs) for classifying encrypted internet traffic. Its focus is on analyzing packet size and inter-arrival times for classifying traffic. SNNs are biologically inspired models that can process information in the form of spikes, much like the human brain. This method achieved a 95.9% accuracy on the ISCX dataset. A type of artificial neural network that often discretely processes inputs is known as a Spiking Neural

Network (SNN). This class of networks has several advantages, one of which is its energy efficiency, even if it processes and transmits data in an event-driven fashion and often uses a lot of energy, particularly when running on neuromorphic hardware. Typical SNNs do a great job of classification, sometimes better than ordinary machine learning models, because they understand complicated patterns as they exist in time. The second benefit of the SNNs is forecasting in real time, which is used in many different cases, especially for life networks. Even though it is hard to optimize the spiking neurons with the ordinary gradient-based methods, the training is more complicated for the ordinary deep learning networks. It requires specific learning techniques, such as spike-timing-dependent plasticity (STDP) or surrogate gradient methods, which require extra computational resources. As such, the hardware requirements have been one of the main factors preventing the distribution of many software applications.

2. Extensible Machine Learning for Encrypted Network Traffic Application Labeling via Uncertainty Quantification

The paper proposes an ML framework that adjusts to new encrypted network traffic using Uncertainty Quantification and Active Learning. It allows the model to regularly retrain itself to ensure it can correctly identify new and unseen traffic patterns. When using the proposed framework, the following benefits are ensured: Flexibility: new types of traffic can be learned without requiring retraining on all other types. This allows for a high level of flexibility in practice. Uncertainty quantification: ensures a high level of accuracy (precision and recall) by only allowing to identify traffic when it is confident. The assessment was performed on 150,000 images of encrypted and plain traffic, and it scored an F1 of 0.98, which means that it worked well for the encrypted network traffic, including VPN-encrypted traffic. Another advantage is that it can be updated in real-time, and the model becomes more and more accurate since the active learning process would allow the model to learn from the environment with time, making it more accurate in the classification of threats. That said, the framework also has its own restrictions. It requires the initial dataset to be comprehensive, which means that if the training dataset is not diverse enough, the framework would be unlikely to generalize well to the new traffic types. Moreover, although it is supposed to be adaptive, it can be computationally expensive to retrain the model, which can be particularly true in real-time applications where the model needs to be updated regularly.

3. Hybrid Feature Learning Framework for the Classification of Encrypted Network Traffic

This paper proposes a hybrid approach combining Support Vector Machines (SVM) and Deep Neural Networks (DNN) for the classification of encrypted network traffic. It leverages DNNs for feature learning to improve the performance of SVMs. The study reports an improved F1 score from 0.78 to 0.90.

The DNN-SVM hybrid model structure is developed to leverage the benefits of DNN and SVM techniques for better performance in traffic analysis classification. Among the benefits, the major one is the increase of accuracy as DNN and SVM are combined to enhance the classification results beyond what they can do alone. This approach copes with class imbalance in the network traffic datasets effectively by using SVM to find optimal decision boundaries in case of a skewed distribution. The model is also scalable and can be extended to handle larger datasets or more complex traffic patterns and can be used in real-life applications as the network data grows. However, the hybrid model has its disadvantages. Specifically, one of the problems is that the hybrid approach is computationally expensive. So, training and utilizing the DNN and SVM components require a large amount of processing power and memory, making it resource-intensive. Another limitation is the complexity of implementation. Specifically, to implement both models and fine-tune them, one must possess deep knowledge of machine learning, optimization, and network traffic analysis to deploy the hybrid model efficiently.

4. Encrypted Network Traffic Classification Based on Machine Learning

This paper compares various machine learning models to classify encrypted network traffic, including using neural networks combined with ensemble methods. The best-performing model achieved 96.8% accuracy in classifying different types of encrypted network traffic. It is an ensemble learning approach that enhances the network traffic classification by employing multiple machine learning techniques to improve accuracy, adaptability, and performance. The best advantage of this approach was that it worked with 96.8% accuracy on a diverse set of traffic types, which proves

that this approach is robust. The next advantage is its flexibility, it can be adapted to any environment and data set, i.e., this approach can be used in the real system. However, another advantage is scalability, this ensemble method can be extended to process a large set of data. At last, it can be used for traffic classification at an enterprise level where there is a large set of data to be analyzed. However, despite the above good points, it has certain disadvantages, one of which is that it is very time-consuming to train multiple classes, and also, it can be computationally very expensive to apply ensemble methods to obtain good results in general. Another disadvantage is that ensemble classifiers are highly dependent on the quality of the data and diversity of the classifiers, i.e. if the initial data set does not have the right representative of real-world traffic, the result is not guaranteed.

5. A Graph Representation Framework for Encrypted Network Traffic Classification

The paper proposes a graph-based model for encrypted network traffic classification. By presenting network traffic in the form of interconnected graphs, the model can hold essential information and the traffic is obfuscated or encrypted. This method outperforms traditional models and especially well with advanced obfuscation techniques. The graph-based approach to network traffic classification is based on the utilization of graph representations to enhance resilience to such obfuscation techniques as encryption. In other words, it is highly effective in complex network environments. One of its key benefits is that it is highly resilient to obfuscation since the graph model captures structural connections within the network traffic, not features that can be easily masked. Moreover it provides high accuracy, the method of packet-level classification shows more than 92%, more than traditional ones, especially if the data is encrypted or obfuscated. Furthermore, the method is robust, as the graph model can capture complicated dependencies between packets, so that it can classify even heavily encrypted traffic better than traditional ones. However, drawbacks of this theory are also present. One of the main problems of graph-based models is computational complexity, as it highly demands for the model to be trained and be used for real-time inference because of the need of large amount of computational power. The method is not generalizable, as its efficiency might depend on the network configuration, especially if the traffic flow is hard to predict. This constricts the method to be used for some real applications.

6. Adversarial Training for Robust Encrypted Traffic Classification

This paper looks at applying adversarial training to make machine learning models more resistant to evasion and obfuscation in encrypted traffic. The authors show that adversarial examples can help the model resist manipulation by obfuscation techniques like VPNs and Tor. The adversarial learning approach is useful in enhancing network traffic classification. This enhancement is achieved by increasing the stability of the model against manipulation techniques such as adversarial attacks and obfuscation. One of its major advantages is that it increases robustness. The model becomes more robust due to adversarial training. This is because it makes it less prone to adversarial or obfuscated attacks. It can also be used for security-critical tasks. This could be the case if the model is used for security-sensitive applications, where robustness to malicious manipulation of traffic is critical. The model is also effective in a variety of settings and scenarios. For example, it can track traffic even when it is obfuscated or encrypted to evade detection. However, there are also some challenges to this approach. The disadvantage is that it makes it necessary to spend more time and computational resources for training. It is so because adversarial training requires generating and using adversarial examples, which increases the burden on the processor. Overfitting may become a problem too, in which the model becomes very specific and is good at detecting adversarial examples but loses the ability to work with general traffic patterns, potentially reducing its real-world utility.

7. Deep Learning for Encrypted Traffic Classification with Small Data

Researching deep learning for encrypted traffic classification is the focus of this paper. The emphasis is on situations where only a small amount of labeled data is available. The research team uses few-shot learning to achieve a high level of classification accuracy using a small amount of data. This approach improves network traffic classification because models can learn well from a very small number of labeled data examples. This is a big advantage because there is often a shortage of labeled traffic data. Even though the model is trained on only a small amount of data, it is still highly accurate, thus working well in a scenario with limited data. Limitations, though, do exist. The quality and diversity of the training dataset must be quite high. If the dataset is not diverse and is of poor quality, the model will not be able to

accurately classify new traffic. Models built with few-shot learning might not scale easily if the dataset is small because they do not work well with a large variety of data. The lack of scalability is a major limitation of the approach, making it less suitable for enterprise-level environments.

8. Federated Learning for Privacy-Preserving Encrypted Traffic Classification

This paper introduces federated learning as a solution for encrypted traffic classification while preserving privacy. The federated approach allows training to occur on local devices, with aggregated updates shared to improve the global model. The federated learning approach enhances network traffic classification by enabling decentralized model training while preserving user privacy. One of the main benefits is that raw traffic data is kept on local devices. This reduces the risk of exposure and makes it possible to meet privacy regulations. In addition, federated learning supports the training of the model in a distributed way, in which the computational power of multiple devices rather than a central server is used, which increases the regularity and reduces the requirement for large data transfers. Yet federated learning has issues of its own. Most significantly, this method is bogged down by its high communication burden because abundant data transmissions are needed to harmonize model updates on fragmented devices. This will likely lessen the speed of learning and create network clogging. Also, complex model aggregation poses a challenge since the correct combination of updates from devices with different abilities and network conditions is likely to result in discrepancies in model training and make optimization more difficult. Despite these issues, federated learning remains a promising method for maintaining network traffic classification privacy and scalability.

9. Traffic Flow Classification Using Transformer Networks for Encrypted Traffic

Research suggests the use of Transformer networks, which are known for their ability to capture long-range dependencies, for classifying encrypted traffic. The study shows that the Transformer outperforms the traditional methods like RNN and CNN in the case of encrypted traffic. The Transformer-based approach for network traffic classification utilizes the self-attention mechanism to analyze the sequences effectively, making it perfect for capturing long-term dependencies in the network traffic flows. Long-range dependency handling is one of the key advantages since Transformers are good at understanding contextual relationships across the entire sequences, which is important for analyzing complex traffic patterns, in particular. Also, this model illustrates the best performance, outperforming traditional RNN and CNN, among the others, particularly in the type of encrypted and highly obfuscated traffic, with which traditional methods face challenges. The Transformer has some drawbacks. The first is high computational cost due to the demands on significant processing power and memory, as well as the need for specialized hardware like GPUs or TPUs for both training and inference. The other is implementation complexity because to fine-tune the Transformer for specific network traffic classification tasks, one must know the model architecture, hyperparameter optimization, and efficient data processing techniques. Despite these challenges, the Transformer remains a powerful tool for network traffic analysis, in particular for scenarios that require a deep understanding of the sequence.

10. Ensemble Learning for Classifying Encrypted Traffic: A Comparative Study

The paper provides a comparison of different ensemble learning methods for encrypted traffic classification: bagging, boosting and stacking. The best accuracy was shown by stacking. Ensemble learning improves the network traffic classification by combining several models to increase accuracy and adaptability. Research indicates usage of Transformer networks, which are effective in capturing long dependencies for encrypted traffic classification. It is proved that the Transformer surpasses traditional methods such as RNN and CNN in the case of encrypted traffic. Transformer-based network traffic classification uses a self-attention mechanism to analyze sequences effectively and it is ideally suited for identifying long dependencies in network traffic flows. Long-range dependency handling is one of the key advantages since Transformers are good at understanding contextual relationships across the entire sequences, which is important for analyzing complex traffic patterns, in particular. Also, this model illustrates the best performance, outperforming traditional RNN and CNN, among the others, particularly in the type of encrypted and highly obfuscated traffic, with which traditional methods face challenges. The Transformer has some drawbacks. The first is high computational cost due to the demands on significant processing power and memory, as well as the need for specialized hardware like GPUs or TPUs for both training and inference. The other is implementation complexity

because to fine-tune the Transformer for specific network traffic classification tasks, one must know the model architecture, hyperparameter optimization, and efficient data processing techniques. Despite these challenges, the Transformer remains a powerful tool for network traffic analysis, in particular for scenarios that require a deep understanding of the sequence.

11. Multi-View Learning for Encrypted Traffic Classification: A New Perspective

The introduction of Multiview learning for encrypted traffic classification is the main topic of this paper. In the paper, several types of features are combined (flow-level, packet-level, and statistical features) to enhance the robustness and accuracy of the model. This approach improves network traffic classification by incorporating different types of features into a more comprehensive representation of network behaviour. One of the main advantages of the approach is that it increases classification performance. Indeed, this approach is going to help the model to capture more complex traffic patterns and, thus, improve the accuracy of classification. The main area of application is to be able to manage different types of traffic, including encrypted and obfuscated flows. However, the main disadvantage of the method is the complexity of the model. In other words, the inclusion of several views will make it more difficult to manage the computational power needed for training and inference. In other words, it will be more complicated to select the right features from different views. This necessitates the use of different methods to select the best features. Despite the disadvantages, it can be said that Multiview learning can be a very useful tool for classifying network traffic in a dynamic environment.

III. Identified Research Gaps:

From the literature review, some key research gaps within the domain of encryption network traffic classification are evident. These gaps can be filled by utilizing novel methods, improving current models, or exploring new avenues. In this analysis, I will describe the research gaps that have been identified and suggest how to close them, including the hints from your research work.

1. Limited Generalization to New Unknown Traffic Types

Research Gap: There are studies that concentrate on well-defined datasets and may face generalization issues in an environment with unknown traffic types. For instance, when new protocols or applications are introduced, the existing models may not help classify them.

How the Gap Can Be Filled:

Uncertainty Quantification and Active Learning: Jorgensen and others' [2] work on Uncertainty Quantification and Active Learning led to the introduction of uncertainty quantification, enabling the model to learn and update itself when met with new, unseen traffic. Extending the method and mixing it with few- shot learning could foster generalization in front of novel traffic.

Scope of the Contribution: It might further explore the use of adaptive and incremental learning techniques, which allow the model to keep updating itself as new traffic types emerge without the need for a full retraining. It could also investigate the use of transfer learning techniques to improve generalization between environments.

2. High Computational Complexity

Research Gap: Advanced models, particularly those using deep learning or graph-based methods (e.g., Okonkwo et al., 2025), usually have high computational overhead and long training times. Thus, these models are hardly suitable for real-time or large-scale deployment, particularly in resource-constrained environments.

How the Gap Can Be Filled:
Model Optimization and Lightweight Architectures: Explorations have been started by researchers in neural network models that are efficient to eliminate the computational complexity without the loss of the accuracy. Model pruning quantization or distillation (or any other work) techniques could be applied to reduce the overhead of deep learning

models.

Hybrid Models: The Hybrid models suggested in the Ramraj and Usha (2023) paper are the models that combine classical machine learning techniques, such as SVMs, with deep learning models. Then, you can study more hybrid methods with fewer

Scope of the Contribution: It can be possible to explore novel resource-efficient models. These models may focus on improving accuracy and efficiency trade-offs. It is necessary to investigate the deployment of such models on edge devices or distributed systems. This can increase scalability and reduce computational costs.

3. Difficulty in Handling Obfuscated or Encrypted Traffic

Research Gap: Traffic obfuscation techniques like VPNs, proxies, and Tor are becoming more common, and they present challenges to existing traffic classification models, which often fail to detect or classify such traffic correctly. This issue is especially challenging for traditional feature-based models that rely on visible patterns in traffic data.

How the Gap Can Be Filled:

Adversarial Training: Okonkwo et al. (2025) is endowed for the paradigm of the traffic representation by the graphs that can be invulnerable to both the encryption and the obfuscation. Such a method is able to capture the very essence of the traffic and make it less dependent on the changes in the packet structure and the traffic flow.

Graph-based Models: Okonkwo et al. (2025) propose graph-based representations of traffic, which could be robust to encryption and obfuscation. This approach captures the intrinsic structure of traffic, making it less susceptible to changes in the packet structure or traffic flow.

Scope of the Contribution: If this were an article, one could consider discussing the hybrid model exploration. The hybrid model that mixes adversarial training with graph-based representations may help the model deal with standard and obfuscated traffic types more efficiently.

4. Privacy and Data Security Concerns

Research Gap: Privacy concerns are becoming a significant issue when collecting and analyzing network traffic data. Existing models may compromise privacy by requiring the use of raw traffic data for training purposes. Moreover, federated learning, although promising, still faces challenges in terms of model aggregation and communication overhead.

How the Gap Can Be Filled:

Federated Learning and Differential Privacy: Federated learning, as discussed by Park et al. (2024), appears to be a hopeful prospect for tackling the issue of privacy-preserving traffic classification. However, to make it more secure, it could be a good idea to implement differential privacy during training to make sure that no user-sensitive information is revealed while the model still learns effectively.

Encrypted Traffic Processing: Another way could be developing privacy-preserving models that operate on encrypted data without needing to decrypt it. This will ensure that no sensitive data will be exposed to the world during the classification process.

Scope of the Contribution: The primary area of concentration is enhancing the mechanisms for preserving privacy in models for classifying traffic by means of leveraging the techniques of federated learning and differential privacy. Besides, you can consider exploring the ways to classify the encrypted traffic without decrypting it to be the main task for your work.

5. Overfitting to Small Datasets

Research Gap: Many models in the literature (like those using deep learning) tend to overfit to small or imbalanced datasets, especially in cases where the number of labeled examples is limited. This issue is particularly relevant when classifying new types of encrypted traffic, which may not have enough labeled data for training.

How the Gap Can Be Filled:

Few-shot and Zero-shot Learning: The approach used by Tsai et al. (2023) in handling small data via few- shot learning is highly effective. Expanding this approach to work in a zero-shot scenario, where the model can classify traffic it has never seen before, could be a groundbreaking direction.

Data Augmentation: Techniques for augmentation of data are capable of solving under label problem. One of the most efficient techniques is data synthesis. It can generate encrypted traffic patterns, mimicking realistic traffic. This can be achieved with varying packet sizes or timings.

Scope of the Contribution: To extend the current research, a possible approach is to put extra emphasis on creating innovative strategies for data augmentation. The other path to consider could be constructing few- shot and zero-shot learning models that would be efficient with small datasets. Such solutions will be especially useful in environments with a lack of labeled data.

6. Model Interpretability

Research Gap: Most of the updated machine learning models that include deep learning models are often portrayed as the so-called "black box," which implies the absence of a clear understanding of why certain traffic is classified in a particular way. This can be a real obstacle in cybersecurity when transparency and explainability are required.

How the Gap Can Be Filled:

Explainable AI (XAI) Approaches: Explainability can be integrated into machine learning models, which could assist users and security professionals in understanding the reasons for the decisions that are made. Techniques such as SHAP and LIME can be used to help explain why a particular traffic sample was classified a certain way.

Hybrid Models for Interpretability: Deep learning architectures can be merged with traditional machine learning methods like decision trees and SVMs. The results are transparent and high performing.

Scope of the Contribution: The incorporation of explainability in your model might be a good idea. Furthermore, this is especially relevant in sensitive settings like network security, as the understanding of the model's decision-making process is indeed very crucial. Moreover, even in other scenarios, you would want to have a sense of trust and transparency in your models. This can be done with techniques such as SHAP or LIME.

IV. Conclusion

In this paper, the survey has studied the current state of encrypted network traffic classification, reviewed significant progress in this field, and identified the main gaps in research. Literature indicates an increasing need for models that can be well generalized for new types of traffic, can reduce computational complexity, can handle obfuscating or encrypted traffic, can preserve privacy, and can avoid overfitting on small datasets. The gaps indicated the significant problems in the implementation of effective and efficient traffic classification systems, especially with the emergence of more sophisticated encryption and obfuscation methods. Conducting a broad literature review allowed the study to identify several potentially promising ways to solve these problems. These include unsupervised quantification, active learning, adversarial training and hybrid models. In addition, techniques such as federated learning, few-shot learning and model explanation are essential for improving model performance and privacy interpretation. The use of existing methods allows you to significantly mitigate these difficulties. The research presented in this work allows understanding the direction in which further work should be done in order to make the traffic classification models obtained as reliable, efficient and flexible as possible. Future research has to focus on building models capable of adapting to new challenges, achieving better generalization in different environments, as well as addressing security and privacy issues. In conclusion, it is possible to build next-generation models of traffic classification by addressing the identified gaps in research. Such models will not only be more accurate, but they will also be more resilient to encryption, hiding techniques, and adversarial attacks. Therefore, it will be possible to build a more effective system of network monitoring and security in conditions of the increasing encryption of the Internet.

Reference

[1] Ali Rasteh, Florian Delpech, Carlos Aguilar-Melchor, Romain Zimmer, Saeed Bagheri Shouraki, Timothée Masquelier (2021), Encrypted Internet Traffic Classification Using a Supervised Spiking Neural Network. https://doi.org/10.1016/j.neucom.2022.06.055.

[2] Steven Jorgensen et al.(2023), Extensible Machine Learning for Encrypted Network Traffic Application Labeling via Uncertainty Quantification. https://doi.org/10.1109/TAI.2023.3244168.

[3] S. Ramraja and G. Usha (2023), Hybrid Feature Learning Framework for the Classification of Encrypted Network Traffic. http://dx.doi.org/10.1080/09540091.2023.2197172.

[4] Wei Lin, Yu Chen (2024), Robust Network Traffic Classification Based on Information Bottleneck Neural Network. http://dx.doi.org/10.1109/ACCESS.2024.3477466.

[5] M. Tsai, L. Chen, J. Lee (2023), Deep Learning for Encrypted Traffic Classification with Small Data. https://doi.org/10.1016/j.comnet.2023.109648.

[6] S. Kumar, N. Soni, M. Mishra (2023), Ensemble Learning for Classifying Encrypted Traffic: A Comparative Study.

[7] F. Wang, L. Chen, X. Wu (2024), Traffic Flow Classification Using Transformer Networks for Encrypted Traffic. https://doi.org/10.3390/app15062977.

[8] J. Park, S. Lee, M(2024). Federated Learning for Privacy-Preserving Encrypted Traffic Classification

[9] Reham Taher Elmaghraby et al (2024), Encrypted Network Traffic Classification Based on Machine Learning. https://doi.org/10.1016/j.asej.2023.102361.

[10] H. Chen, S. Wang, Y. Zhang (2025), Multi-View Learning for Encrypted Traffic Classification: A New Perspective

[11] Zulu Okonkwo et al (2025), A Graph Representation Framework for Encrypted Network Traffic Classification. https://doi.org/10.1016/j.cose.2024.104134.