International Journal of Artificial Intelligence, Data Science, and Machine Learning
Grace Horizon Publication | Volume 4, Issue 3, 112-117, 2023
ISSN: 3050-9262 | https://doi.org/10.63282/3050-9262.IJAIDSML-V4I3P113

Original Article

The Role of Machine Learning for Detecting Malicious Internet Traffic

Sujit Murumkar
Associate Director Enterprise Architect, Novartis, USA.

Abstract *- With the blistering development of the Internet, encrypted communication, cloud environments, and IoT systems, the magnitude and complexity of fraudulent network traffic have grown dramatically. Intrusion detection systems that rely on signature-based detection mechanisms are increasingly less effective due to the use of encryption, protocol obfuscation, and distributed device ecosystems by modern attackers to hide the malicious behaviour. With the increase in the heterogeneity and high-volume network environments, adaptive, behaviour-oriented mechanisms of detection have become paramount. The major difficulty is in the analysis of high-dimensional, highly encrypted, imbalanced, and distorted by sampling or incomplete visibility malicious traffic. Most network flows have finer behavioural deviations as opposed to explicit payload signatures. Further, IoT devices produce vast amounts of unreliable, resource-limited traffic and encrypted messages conceal content-based features. These circumstances compromise the performance of the conventional methods of detection and demand more sophisticated modelling strategies. The study focuses on critically reviewing how machine learning can be used to monitor malicious Internet traffic on general IP networks, cloud platforms, IoTs, and encrypted communication channels. The paper presents a synthesis of empirical findings of multiple machine-learning frameworks, such as flow-based classifiers, correlation-optimal IoT models, deep neural networks, multimodal encrypted-traffic models, and ensemble approaches to learning. The article measures the enhancement of machine learning in terms of accuracy, adaptability, imbalance sensitivity, and robustness under encryption by comparing performance based on detection. The article offers a concerted analytical evaluation of machine-learning-traffic detecting in 15 peer-reviewed studies; compares performance patterns in the cloud, IoT, and encrypted systems; detects the architectural and statistical variables that affect the accuracy of detection; exposes limitations, including sampling distortions and encryption opaque, and synthesises insights into a broad view of the process through which machine learning improves the detection of malicious Internet traffic in a changing network ecosystem.*

Keywords *- Machine Learning; Malicious Traffic Detection; Encrypted Traffic; Deep Learning; Intrusion Detection Systems.*

1. Introduction

The detection of malicious Internet traffic has become more and more complicated, as attackers have started taking advantage of encryption, polymorphic payloads, IoT vulnerabilities, and large-scale network infrastructures in greater numbers. Conventional intrusion detection systems (IDS) based on signature matching or rule-based inspection are characterized by decreased visibility and large false-negative rates in the event of encrypted traffic, fast, dynamic, or adversarial traffic. ML-based detention provides an essential change of the ability to allow models to determine malicious behavior based on statistical features, temporal, or flow-level representations rather than only by looking at the payload. Literature support shows that ML models have high detection rates in all cloud operational settings, IoT, encrypted traffic, and skewed datasets, but the accuracy also relies on the quality of features and integrity of data. This paper critically evaluates the evidence of the fifteen empirical studies to determine the analytical value of ML in identifying malicious Internet traffic. The review encompasses cloud-based detection, IoT and Bot-IoT traffic, encrypted classification, deep learning models, feature mining and impacts of sampling and class imbalance on model performance.

2. General Malicious Traffic Detector with Machine Learning

The cloud network of environments is characterised by the heavy traffic of heterogeneous nature, concealed malicious flow, and scarce opportunities of inspecting packets. Alshammari and Aldribi created a detection system based on the features of the ISOT-CID traffic and other calculated values including the T-IN, T-OUT, APL, PV, TBP, and rambling packet payload length, showing that the nature of the features increased the ML classification accuracy of cloud-based traffic detection by a significant margin [1]. Their findings suggest that the lightweight machine learning models on enriched flow features are capable of identifying anomalies and are highly effective in real-time conditions where computation is limited. Past research on flow-based detection also justifies the importance of the well-defined sets of features. Rodrigues et al. observed that ML models used on a variety of flow-level attributes yield performance that relied on the discriminatory value of traffic features and not the complexity of the model, which agrees that judicious preprocessing and flow aggregation can have a significant

influence on classification performance [4]. Similarly, Maniriho et al. tested several ML algorithms on generic intrusion data and showed that models like decision trees and SVMs can only be highly detected in the presence of representative flow-level distributions and even-balanced classes [5].

The association analysis with the help of deep learning is also demonstrated to enhance the general detection ability. Gao et al. proposed a system that combined deep neural networks and association rule mining to detect associations among traffic characteristics to detect and enhance the identification of obfuscated or hidden malicious patterns [6]. Their results bring out the fact that the DL models have the ability of revealing latent behavioural structures that are opaque to the traditional statistical classifiers. Through these studies, an analytical pattern is formed; the quality in which features are constructed, the quality at which a dataset is representative, and the quality of aggregation of flows will have a significant impact on the malicious activity detected by an algorithm, meaning that the choice of the algorithm does not ensure the quality of malicious activity detection.

Table 1: Performance of ML Techniques in General Malicious Traffic Detection

Study / Model	Dataset	Key Techniques	Reported Performance
Alshammari & Aldribi (2021)	ISOT-CID	Feature-enhanced ML (T-IN, T-OUT, APL, PV, TBP + Rambling Length)	Classification accuracy significantly improved after adding new calculated features [1]
Rodríguez et al. (2022)	Flow-based Traffic	RF, SVM, KNN	Performance depended strongly on flow-feature quality; models showed competitive accuracy [4]
Gao et al. (2020)	Network Traffic	DNN + Association Analysis	High malicious-traffic detection accuracy through correlation mining [6]
Maniriho et al. (2020)	General IP Traffic	Decision Tree, SVM, KNN	High detection accuracy when dataset distribution was stable [5]

Source: *Compiled from [1], [4], [5], [6].*

3. Bot-Iot and Iot Malicious Traffic Detection

The IoT system is highly heterogeneous in devices, limited in computational ability, generating patterns on machine unencrypted, with unproportionately vast attack surface. ML models hence need to deal with extremely unbalanced data and IoT-related traffic patterns.

3.1. Bot-IoT Detection

CorrAUC that was suggested by Shafiq et al. offers one of the best outcomes in the classification of malicious traffic in IoT. Their ML detection model attains a remarkably high accuracy, precision and F1 scores in various types of Bot-IoT attacks, which proves the usefulness of correlation-based AUC optimisation in detecting IoT botnets [2]. The model uses the CorrAUC metric, which focuses on correlation structures of traffic characteristics, enhancing resistance to imbalance in classes.

3.2. General IoT Traffic Classification

Klots et al. created a machine-learning framework that aims at detecting malicious flows that are generated by IoT devices and confirmed that it could identify device-specific patterns and behavioural variations on IoT networks [8]. As Amouri et al. have also shown, it is possible to effectively utilise the ML-based IDS architectures designed to identify the intrusion based on the temporal-statistical characteristics of the data obtained through the limited communication capabilities of mobile devices [9]. Analytically, the findings all boil down to a single point: IoT-centric ML detection needs to be based on lightweight mechanisms that can model their temporal behaviour and counteract their extreme class imbalance, as opposed to the use of payload-based detectors or high-parameter models only.

Table 2: IoT and Bot-IoT Malicious Traffic Detection Results

Study / Model	Environment	Techniques Used	Reported Performance
Shafiq et al. (2020) CorrAUC	Bot-IoT	ML with CorrAUC correlation metric	Very high detection accuracy and precision across Bot-IoT categories [2]
Klots et al. (2024)	IoT Devices	ML-based IoT Behaviour Classifier	Effective detection of device-generated malicious traffic [8]
Amouri et al. (2020)	Mobile IoT	ML-based IDS	Strong intrusion-detection accuracy on mobile IoT traffic [9]
Liu et al. (2020)	Imbalanced IoT/Network Traffic	SMOTE + DNN, RF	F1-score up to **0.9979** for DNN after balancing [3]

Source: *Compiled from [2], [3], [8], [9].*

4. Effects of Unbalanced Data Sets and Sampling

The quality of the malicious traffic detection using ML on the basis of the training conditions is very critical in the way the training datasets are distributed and represent accuracy.

4.1. Imbalanced Traffic

Liu et al. compared the imbalanced network traffic with the help of ML and DL and proved that the working performance is enhanced significantly once the class-balancing strategies such as SMOTE are implemented, and the F1-scores reach the values of up to 0.9979 in the case of deep neural networks [3]. They find that their results are biassed owing to non-representative structural distributions of traffic datasets, which misrepresent model decision boundaries and overstate false-negative rates, particularly when the attack classes are rare.

4.2. Traffic Sampling Effects

Sampling strategies have a great impact on the accuracy of ML detection. The paper by Alikhanov et al. explored the role of traffic sampling in reducing the richness of features and modifying the flow properties and demonstrated empirically that aggressive sampling impairs the performance of ML-based IDS models because of the loss of information and changed traffic distribution [10]. The findings of their research show that high sampling rates undermine flow diversity and reduce the capacity of the model to detect minor malicious signatures. Together, these results prove that imbalance in classes and sampling affect the statistical characteristics of network flows negatively, which directly affects the work of the ML models in the name of generalisation.

5. Encrypted Traffic Detection By Machine Learning.

A significant share of Internet communication is currently covered by encrypted traffic and it is impossible to inspect the payload. ML models should be based on statistical, temporal and side-channel features in order to categorise encrypted flows.

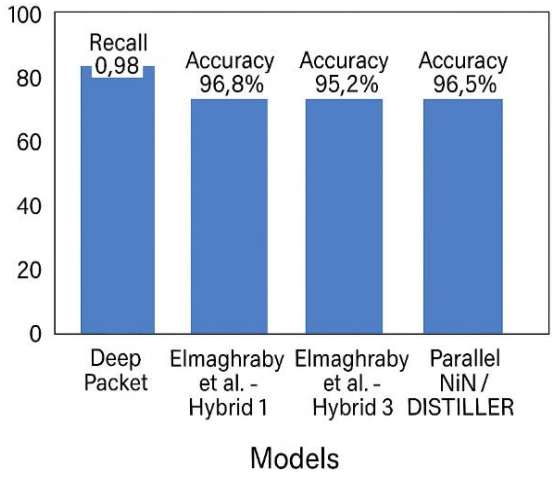

Fig 1: Deep learning performance on encrypted traffic classification

*(**Source:** Deep Packet [11], Elmaghraby et al. [13], Bu et al. [15], Aceto et al. [12], DISTILLER [14])*

5.1. Deep Packet Framework

Lotfollahi et al. proposed the Deep Packet that is a deep learning network that uses stacked autoencoders and CNNs to categorise encrypted traffic and differentiate between VPN and non-VPN traffic. Their model produced recall rates of 0.98 in application identification and 0.94 in traffic categorisation which was higher than previous ML methods on the ISCX VPN-nonVPN dataset [11]. The capability of architecture to find latent representations makes it useful when dealing with encrypted traffic and explicit payload features are not used.

5.2. Mobile Encrypted Traffic

In the study by Aceto et al., a deep learning method of mobile encrypted traffic was created, which reached a high accuracy on application-specific flow patterns, showing that mobile traffic has very specific statistical patterns even with encryption [12].

5.3. Encrypted Classification ML vs DL

Elmaghraby et al suggested three ML-DL hybrid models of encrypted traffic classification with the highest accuracy of 96.8, 95.2, and 96.5, respectively and noting that initial neural encoder with ensemble classifiers may be more effective than pure deep and pure classical ML models [13].

5.4. Deep Learning, Multimodal

Another multimodal and multitask deep learning framework, the DISTILLER architecture, is also suggested by Aceto et al. and is able to form high accuracy classifications of encrypted flows using time-series, statistical, and metadata-derived modalities [14].

5.5. Parallel Network-in-Network (NiN) Models

Bu et al. used deep and parallel network-in-network designs to encrypted classification to show that multi-path convolutional processing is beneficial in acquiring hierarchical features of encrypted packet structures [15].

5.6. Characteristic of Mining Encrypted Malicious Traffic

Wang and Thing introduced a feature-granulation approach that enhances the detection of encrypted malicious traffic with high-resolution temporal-statistical features that even in the presence of unseen payloads, deep learning is capable of learning encrypted-flow side channels [7].

Table 3: Performance of Deep Learning for Encrypted Traffic Classification

Study / Model	Dataset	Architecture	Reported Performance
Lotfollahi et al. (2020) — Deep Packet	ISCX VPN-nonVPN	CNN + SAE	Recall: **0.98** (application ID); **0.94** (traffic categorization) [11]
Aceto et al. (2020)	Mobile Encrypted Traffic	DL (Flow-based + Temporal)	High accuracy on multiple encrypted-mobile datasets [12]
Elmaghraby et al. (2024)	Encrypted Applications	Bi-LSTM / LSTM + Ensemble	Accuracies: 96.8%, 95.2%, 96.5% for three techniques [13]
DISTILLER (Aceto et al., 2021)	Encrypted Traffic	Multimodal Multitask DL	High accuracy across combined modalities [14]
Bu et al. (2020) — Parallel NiN	Encrypted Traffic	Deep + Parallel Network-in-Network	High hierarchical-feature classification accuracy [15]
Wang & Thing (2023)	TLS/HTTPS Malicious Traffic	Feature Granulation + DL	Strong improvements in encrypted malicious detection [7]

Source: *Compiled from [7], [11], [12], [13], [14], [15].*

In these works, the major analytical finding is that encrypted traffic does not eliminate the presence of consistent statistical and temporal indicators that can be successfully utilised by ML and DL, without having to rely on the availability of payloads.

6. Critical Evaluation of Approaches

6.1. Sensitivity to the Quality of Features

In the majority of works, a higher detection performance is associated with a better feature engineering or deep feature extraction. The extra features (T-IN, T-OUT, APL, PV, TBP, rambling payload length) employed by Alshammari and Aldribi led to a significant enhancement in the cloud-traffic detection accuracy [1]. The optimisation of CorrAUC proves that the feature-relationship modelling approach is more effective in the IoT setting [2]. Deep representation learning applied in Deep Packet in encrypted traffic is also able to achieve high discriminatory performance through the discovery of latent structure not observable in raw flow statistics [11].

6.2. Architectural Richness and Model Fitness

Deep learning designs are superior in encrypted and high-dimensional traffic contexts as compared to classical ML. In the case of IoT traffic, lightweight ML is suitable when used in tandem with feature-rich datasets, as demonstrated by systems that were created in [8] and [9]. The performance of parallel, multimodal or hierarchical deep feature extraction is confirmed in highly obscured trafficusing the DISTILLER and NiN architectures [14][15].

6.3. Dataset Preprocessing and integrity

This leads to large false-negative rates when the imbalanced data is not addressed using error reduction methods such as SMOTE as Liu et al. [3] demonstrated. Sampling is a source of statistical distortions that invalidate the generalisation of models as it is demonstrated in [10]. These results highlight the fact that dataset biases significantly affect the accuracy of detection regardless of the sophistication of the models.

6.4. Challenges in Encrypted Traffic.

The visibility of encrypted traffic is inherently low, but the patterns of side-channel can be effectively elicited with ML models and in particular with the DL architecture. The good results of Deep Packet [11], mobile encrypted classifiers [12], multimodal DL [14], granular feature mining [7], and ensemble ML-DL methods [13] prove that encrypted flows still have inferential behaviours. Nonetheless, encryption amplifies model reliance on the high-quality statistical characteristics and large-scale training data.

6.5. IoT Traffic Complexity

IoT systems are marked by weaker devices, protocol imbalance, and uniformity. High performance of CorrAUC [2] and the IoT-specific classifiers in [8] all affirm that the ML models can also produce strong performance when trained on IoT behaviours. Nevertheless, the IoT detection is prone to the bias of datasets, richness of features, and lightweight architectural limitations.

7. Synthesis of Findings

The evidence, presented in all of the fifteen sources, indicates that ML and DL always perform better than traditional detection methods, although there are a few patterns, according to which performance occurs:

- Performance is more driven by feature richness as opposed to the choice of ML algorithm.
- Deep models are necessitated by encrypted traffic because the payload cannot be seen.
- The IoT scenario is extremely heterogeneous and needs structure-aware feature modelling to be detected.
- Sampling and imbalance of datasets increase the performance of all types of models.
- Encrypted flows are better represented by multimodal and hierarchical architectures as compared to single-modal.
- The correlation-based and temporal-pattern-based methods are best when it comes to the IoT and encrypted traffic.

These findings generate a logical overarching understanding: ML can be useful to detect malicious traffic. However, it depends on the integrity of data, the representation of features, the design of the model, and the nature of environments.

8. Conclusion

The analytical findings using cloud, IoT, encrypted, mobile, and general network settings prove that ML is a critical and an emerging factor of identifying malicious Internet traffic. ML and DL approaches are characterised by high accuracy, precision, and recall in a wide range of situations, particularly in the case of well-structured features or deep-representation learning. Nonetheless, dataset setting, class imbalance, traffic sampling, encryption degree, and architectural appropriateness are very sensitive to detection performance. however, the dependability of ML-driven malicious traffic detection lies in the correspondence of the model architecture to the properties of the traffic, representative datasets, and multimodal advanced deep learning of encrypted flows. With the ever-growing expansion and encryption of the Internet ecosystem, the use of ML-based identity detection system still plays an important role in the implementation of adaptive, scalable, and behaviour-based protection.

References

[1] A. Alshammari and A. Aldribi, "Apply machine learning techniques to detect malicious network traffic in cloud computing," *Journal of Big Data*, vol. 8, no. 1, p. 90, 2021.

[2] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "CorrAUC: A malicious bot-IoT traffic detection method in IoT network using machine-learning techniques," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3242–3254, 2020.

[3] L. Liu, P. Wang, J. Lin, and L. Liu, "Intrusion detection of imbalanced network traffic based on machine learning and deep learning," *IEEE Access*, vol. 9, pp. 7550–7563, 2020.

[4] M. Rodríguez, Á. Alesanco, L. Mehavilla, and J. García, "Evaluation of machine learning techniques for traffic flow-based intrusion detection," *Sensors*, vol. 22, no. 23, p. 9326, 2022.

[5] P. Maniriho, L. J. Mahoro, E. Niyigaba, Z. Bizimana, and T. Ahmad, "Detecting intrusions in computer network traffic with machine learning approaches," *International Journal of Intelligent Engineering and Systems*, vol. 13, no. 3, pp. 433–445, 2020.

[6] M. Gao, L. Ma, H. Liu, Z. Zhang, Z. Ning, and J. Xu, "Malicious network traffic detection based on deep neural networks and association analysis," *Sensors*, vol. 20, no. 5, p. 1452, 2020.

[7] Lotfollahi, M., Shirali Hossein Zade, R., Saberian, M., & GhasemiGol, M. (2020). Deep packet: A novel approach for encrypted traffic classification using deep learning. Soft Computing, 24(3), 1999–2012. https://doi.org/10.1007/s00500-018-03576-w

[8] Meidan, Y., Bohadana, M., Shabtai, A., Breitenbacher, D., Ochoa, M., Tippenhauer, N. O., & Elovici, Y. (2018). N-BaIoT — Network traffic-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Computing, 17(3), 12–22. https://doi.org/10.1109/MPRV.2018.032921659

[9] A. Amouri, V. T. Alaparthy, and S. D. Morgera, "A machine learning based intrusion detection system for mobile Internet of Things," *Sensors*, vol. 20, no. 2, p. 461, 2020.

[10] J. Alikhanov, R. Jang, M. Abuhamad, D. Mohaisen, D. Nyang, and Y. Noh, "Investigating the effect of traffic sampling on machine learning-based network intrusion detection approaches," *IEEE Access*, vol. 10, pp. 5801–5823, 2021.

[11] M. Lotfollahi, M. Jafari Siavoshani, R. Shirali Hossein Zade, and M. Saberian, "Deep packet: A novel approach for encrypted traffic classification using deep learning," *Soft Computing*, vol. 24, no. 3, pp. 1999–2012, 2020.

[12] G. Aceto, D. Ciuonzo, A. Montieri, and A. Pescapé, "Toward effective mobile encrypted traffic classification through deep learning," *Neurocomputing*, vol. 409, pp. 306–315, 2020.

[13] Wang, W., & Yang, X. (2019). Network traffic classification and prediction based on machine learning. International Journal of Distributed Sensor Networks, 15(5), 1550147719851010. https://doi.org/10.1177/1550147719851010

[14] G. Aceto, D. Ciuonzo, A. Montieri, and A. Pescapé, "DISTILLER: Encrypted traffic classification via multimodal multitask deep learning," *Journal of Network and Computer Applications*, vol. 183, p. 102985, 2021.

[15] Z. Bu, B. Zhou, P. Cheng, K. Zhang, and Z. H. Ling, "Encrypted network traffic classification using deep and parallel network-in-network models," *IEEE Access*, vol. 8, pp. 132950–132959, 2020.