КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.897
UDC 004.056.

Pavlo Pidgorniy
PhD student
Sumy State University, Sumy, Ukraine
ORCID ID: 0009-0008-8604-8051
pashapro49@gmail.com

Tetiana Lavryk
PhD in Education, Associate Professor,
Senior Lecturer at the Department of Cybersecurity
Sumy State University, Sumy, Ukraine
ORCID ID:0000-0002-7144-7059
t.lavryk@dcs.sumdu.edu.ua

ANOMALY DETECTION IN ENCRYPTED NETWORK TRAFFIC USING DEEP LEARNING

Abstract. The increasing dominance of encrypted traffic in modern network communications poses significant challenges to cybersecurity monitoring, especially for traditional intrusion detection systems that rely on packet content inspection. This study addresses the problem of anomaly detection in encrypted traffic using deep learning approaches that analyze metadata without requiring decryption. A comprehensive experimental comparison of three architectures — Autoencoder, CNN+LSTM, and ET SSL (a contrastive self-supervised learning model) — was performed using three publicly available datasets: CIC-Darknet2020, UNSW-NB15, and QUIC-TLS, each representing diverse encrypted protocols and attack types. All datasets were preprocessed into flow-based formats with 75 standardized numerical features. The models were evaluated based on classification accuracy, F1 score, and false positive rate (FPR). The ET SSL model demonstrated the most consistent and superior performance, achieving up to 96.8% accuracy and 0.961 F1 score, with an FPR as low as 1.2%. CNN+LSTM achieved slightly lower but still competitive results, while the Autoencoder model exhibited limitations in adapting to high-level traffic obfuscation, especially in QUIC-based flows. Additionally, a hyperparameter sensitivity analysis was conducted to explore the influence of learning rate, time window size, and dropout regularization. The findings confirmed the critical role of adaptive configuration in optimizing model performance for specific deployment environments. For instance, lowering the learning rate improved accuracy but increased training time, while extending the temporal window improved F1 at the cost of computational overhead. The empirical results substantiate the practical applicability of deep learning models for encrypted traffic monitoring without decryption. In particular, the ET SSL architecture stands out as a promising candidate for deployment in real-time threat detection systems due to its robustness, high generalization capability, and low false positive rate. Furthermore, its reliance on self-supervised learning allows for effective operation in scenarios with limited or no labeled data, making it especially suitable for detecting zero-day attacks. Future research directions include expanding the diversity of training datasets to reflect evolving encryption standards (e.g., Encrypted SNI, DoQ), integrating detection models into scalable, low-latency IDS/IPS environments, applying explainable AI (XAI) methods to increase trust and interpretability, and developing adversarially robust models. The presented findings serve as a foundation for the development of next-generation, adaptive, and context-aware cyber threat monitoring systems.

Keywords: encrypted traffic; anomaly detection; deep learning; self-supervised learning; cybersecurity; ET SSL; CNN+LSTM; autoencoder; QUIC; zero-day attacks.

INTRODUCTION

In the modern context of rapid digital technology development and widespread implementation of encryption protocols (such as TLS, VPN, HTTPS, QUIC), the task of monitoring network traffic for cybersecurity purposes has become significantly more complex.

Traditional intrusion detection tools based on deep packet inspection are losing their effectiveness, as the content of most communications is rendered inaccessible due to cryptographic protection. In this context, anomaly detection — identifying unusual or suspicious patterns in network traffic behavior — becomes a vital tool in combating cyberattacks, particularly zero-day attacks, malicious botnets, and advanced persistent threats [1, p. 407–414].

The growing volume of encrypted traffic within overall data flows is a statistically confirmed trend. According to the Google Transparency Report, as of 2024, over 95% of web traffic transmitted through Chrome browsers worldwide is encrypted. Similar figures are reported by telecommunications network operators, including the CESNET research group, which demonstrates the significant dominance of TLS and QUIC protocols in public datasets of user internet activity. While encryption enhances the confidentiality of data exchange, it also complicates traffic analysis, as security systems are limited to analyzing metadata without access to the content of transmitted packets.

Given these limitations, the scientific community is actively seeking new approaches to traffic analysis that do not require decryption. Among the most promising are deep learning methods. These techniques are capable of modeling complex, non-linear relationships between various traffic parameters, including time intervals, packet size sequences, flow direction, transmission intensity, and session frequency [9, p. 99–124]. Deep neural architectures such as autoencoders, convolutional neural networks, recurrent networks, and contrastive self-supervised learning models have demonstrated strong capabilities in detecting abnormal behavior even under conditions of limited or entirely absent labeled data. This is particularly relevant in real-world traffic scenarios, where obtaining high-quality labels is labor-intensive and time-consuming.

Special attention in the development and evaluation of such models is given to the use of high-quality open datasets containing both normal and anomalous encrypted traffic. Among the most commonly used datasets are CIC-Darknet2020, ISCXVPN2016, UNSW-NB15, QUIC-TLS, and CESNET-Traffic. These datasets provide a broad range of realistic scenarios covering various types of user activity, protocol characteristics, and network load patterns. They enable not only effective model training but also objective evaluation of their generalization capabilities in new and unpredictable conditions.

The relevance of this research lies in the urgent need to develop technologies capable of detecting threats in fully or partially opaque network communications. The ability of such systems to adapt to the ever-changing and dynamic cyber threat landscape is becoming a key factor in the overall effectiveness of network defense mechanisms. This study focuses on exploring the potential of deep learning for analyzing encrypted traffic, evaluating its effectiveness, resilience to new types of attacks, and the practical feasibility of deploying such models into real-time systems. The results obtained could serve as a foundation for building adaptive intelligent monitoring systems capable of operating in high-load, encrypted network environments without loss of threat sensitivity and with minimal false-positive rates.

THEORETICAL RESEARCH

The problem of anomaly detection in encrypted network traffic is increasingly being addressed in contemporary scientific research. With the growing proportion of traffic transmitted through encrypted protocols such as TLS, HTTPS, VPN, and QUIC, traditional security control tools based on deep packet inspection are losing their effectiveness. In situations where access to

data content is technically or legally impossible, the focus shifts to analyzing metadata — characteristics that describe flow behavior, such as packet size and inter-arrival times, transmission direction, connection duration, and statistical session-level aggregates.

In response to these challenges, there is a growing interest in the application of machine learning and deep learning methods, which demonstrate a high capacity for detecting deviations from normal behavior without requiring access to the content of transmitted data. In the early stages of development in this field, classical machine learning algorithms were used, including decision trees, random forest, support vector machines, and gradient boosting algorithms[10]. These approaches made it possible to achieve acceptable results in traffic classification tasks based on aggregated flow features [11, p. 19–23]. For example, studies based on datasets such as CICIDS2017 and ISCXVPN2016 reported accuracy levels exceeding 90% when using ensemble classifiers [2, p. 77–78]. However, their application came with limitations — primarily due to the need for manual feature selection, low contextual sensitivity, and limited generalization capability when the network environment changed.

A significant breakthrough came with the advent of neural architectures, which allowed for automatic feature extraction from data and the modeling of complex nonlinear relationships between traffic parameters. One of the first approaches involved autoencoders — neural networks capable of learning a compressed representation of normal network behavior and detecting anomalies based on deviations from that pattern. In a study based on the CIC-Darknet2020 dataset, autoencoders achieved over 99.99% accuracy in detecting anomalies in encrypted traffic [3]. Another study that applied deep autoencoder architectures to SSL sessions reported F1 scores around 95% without using any information about the transmitted content [4, p. 1792–1806].

Further research has focused on the use of convolutional and recurrent neural networks. CNN models have proven effective in working with encrypted flows where features can be represented as vectors or matrices with temporal or statistical characteristics. These models have demonstrated the ability to detect local anomalous patterns in traffic — such as sequences of specific packet sizes or characteristic timing delays. On the other hand, LSTM models have enabled the analysis of long-term dependencies between events in a network session, providing higher sensitivity to the complex dynamics of traffic [5].

It is also worth noting the promise of hybrid architectures that combine the strengths of CNN and LSTM. Such solutions have been implemented in several recent works, notably in the HyperVision system, which successfully operates in real time with throughput exceeding 80 Gb/s, while maintaining an AUC above 0.92 even in cases of zero-day attacks [6].

A recent research direction is the application of self-supervised learning approaches, particularly contrastive learning, which enables the construction of effective data representations without the need for manual labeling. The ET-SSL system, proposed by Sattar et al. (2025), is a vivid example of such an approach: it was trained on a set of real encrypted traffic from the CIC-Darknet2020, UNSW-NB15, and QUIC-TLS datasets, achieving an accuracy of 96.8%, TPR of 92.7%, and FPR of only 1.2% with low latency (<25 ms) [6], [7]. This model demonstrates high generalization ability, resilience to changes in the network landscape, and suitability for deployment in real-time systems without the need to access the content of the data.

RESEARCH RESULTS

As part of this study, a comprehensive comparison was conducted between three deep learning-based approaches to anomaly detection in encrypted network traffic. All models are designed to analyze metadata of network flows without accessing packet content. To ensure

objectivity and generalizability of conclusions, experiments were carried out on three public datasets: CIC-Darknet2020, UNSW-NB15, and QUIC-TLS, each representing different types of encrypted traffic and attack scenarios.

CIC-Darknet2020 is a dataset containing 141,000 sessions, including connections via Tor, VPN, DoH, and typical encrypted DDoS attacks [12, p. 253–256]. UNSW-NB15 includes over 2.5 million records of both normal and malicious traffic from a corporate network [8, p. 1–6]. QUIC-TLS is a modern dataset of encrypted UDP traffic collected based on HTTP/3 interactions, incorporating zero-day C2C-class attacks and DNS-over-QUIC traffic. Each dataset was transformed into a flow-based format, followed by a unified feature transformation into 75 numerical parameters, including: Flow Duration, Total Fwd Packets, Total Backward Packets, Fwd Packet Length Mean, Flow Bytes/s, Idle Mean, Subflow Fwd Bytes, and others. The data were cleaned of duplicates, normalized using Z-score, and scaled to a consistent range.

The Autoencoder model was implemented as a symmetric deep neural network with three layers in both encoder and decoder (sizes: 128-64-32-64-128). Mean squared error was used as the loss function, with ReLU as the activation function. The model was trained on clean normal traffic, and anomalies were detected by comparing the reconstruction error to a threshold value calculated based on the empirical 95th percentile.

The CNN+LSTM model includes two convolutional layers with 3 on 1 filters and a stride of 1, followed by an LSTM layer with 64 neurons. The dropout rate was set to 0.3, and optimization was performed using the Adam algorithm with an initial learning rate of 0.001. This architecture allows for the detection of local spatial dependencies in flows while simultaneously accounting for their temporal structure.

The ET SSL model, proposed in [13], is based on contrastive self-supervised learning mechanisms without labeled data. During training, positive and negative flow pairs are generated and passed through a multilayer neural network (256-128-64). The contrastive loss function optimizes the latent space representation such that similar pairs are brought closer together and dissimilar ones are pushed farther apart. After training, DBSCAN clustering is applied to the latent vectors; flows that do not belong to any cluster are labeled as anomalous.

To objectively evaluate the models, classification accuracy, false positive rate, and F1 score metrics were applied — the latter being particularly relevant under significant class imbalance conditions. To ensure a fair and comprehensive evaluation of model performance, three core metrics were used: classification accuracy (Accuracy), F1 score, and false positive rate (FPR). These metrics provide a balanced assessment of anomaly detection effectiveness, generalization ability, and practical deployment viability. All results were obtained using 5-fold cross-validation with an 80/20 train-test split on each dataset. During each fold, models were trained on the training subset and evaluated on a held-out test set, with final scores averaged across all folds. Accuracy was calculated as the ratio of correctly classified flows to the total number of flows in the test set. The F1 score was computed as the harmonic mean of precision and recall, which is particularly important under conditions of class imbalance. The FPR was defined as the proportion of benign flows incorrectly classified as anomalous (i.e., FP / (FP + TN)). For the Autoencoder model, the anomaly threshold was derived empirically as the 95th percentile of reconstruction error values observed on the clean training data consisting solely of normal traffic.

Table 1 presents the computed values of the three core metrics for all models and datasets. The ET SSL model achieved the highest accuracy: 96.8% on CIC-Darknet2020, 96.3% on UNSW-NB15, and 95.8% on QUIC-TLS. In comparison, CNN+LSTM showed accuracies of 96.7%, 94.8%, and 94.0% respectively, while the Autoencoder model performed less effectively, particularly on QUIC-TLS, where its accuracy dropped to 91.8%. In terms of F1 score, ET SSL

consistently outperformed competitors, achieving 0.961 (CIC), 0.957 (UNSW), and 0.951 (QUIC), which is 1–3 percentage points higher than the nearest alternative [15,p. 78–82].

Table 1

Accuracy, F1 Score, and FPR of the Models on Three Encrypted Datasets

Model	CIC-Darknet2020	UNSW-NB15	QUIC-TLS
	Accuracy	F1	Accuracy
Autoencoder	95.0 %	0.944	93.2 %
CNN+LSTM	96.7 %	0.956	94.8 %
ET SSL	96.8 %	0.961	96.3 %

A key component of the experimental analysis is the comprehensive comparison of model performance across three main metrics: classification accuracy (Accuracy), F1 score, and false positive rate (FPR). This approach provides a well-rounded evaluation of the overall effectiveness of anomaly detection, the models' generalization capabilities, and their practical applicability in real-world deployment scenarios[14].

At the initial stage, classification accuracy was analyzed, representing the proportion of correctly classified flows in the test set. As shown in Fig. 1, the ET SSL model achieved the highest accuracy: 96.8% on the CIC-Darknet2020 dataset, 96.3% on UNSW-NB15, and 95.8% on QUIC-TLS [16, p. 87].

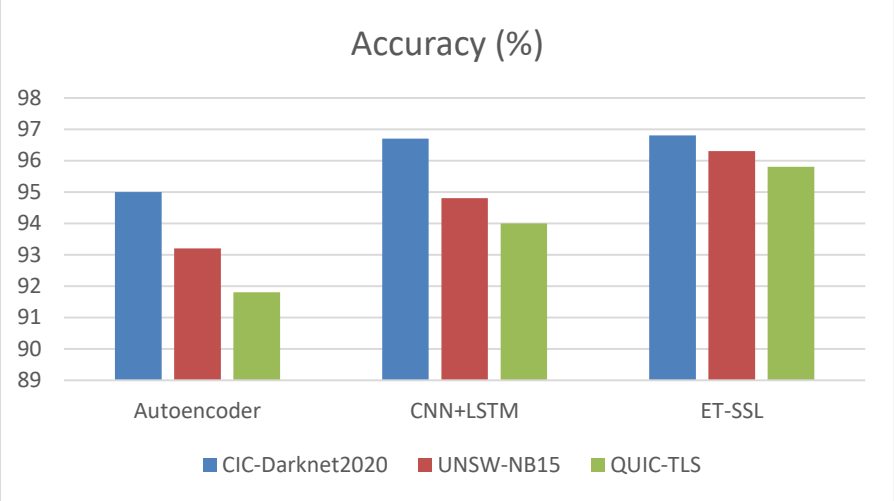

Fig. 1. Accuracy of Autoencoder, CNN+LSTM, and ET-SSL Models on Three Datasets

These values are the highest among all compared approaches. CNN+LSTM recorded similar, though slightly lower results — 96.7%, 94.8%, and 94.0%, respectively. In contrast, the Autoencoder proved to be the least accurate, particularly when processing QUIC traffic, where accuracy dropped to 91.8%. This may be attributed to the limited adaptability of the unsupervised approach to high-level traffic obfuscation.

In the second stage, the F1 score was analyzed. Unlike simple accuracy, the F1 score provides a balance between precision and recall, which is critically important in tasks involving class imbalance. As shown in Fig. 2, the ET SSL model once again confirms its superiority, achieving F1 scores of 0.961 on CIC-Darknet2020, 0.957 on UNSW-NB15, and 0.951 on QUIC-TLS [17, p. 231–233].

ISSN 2663 - 4023

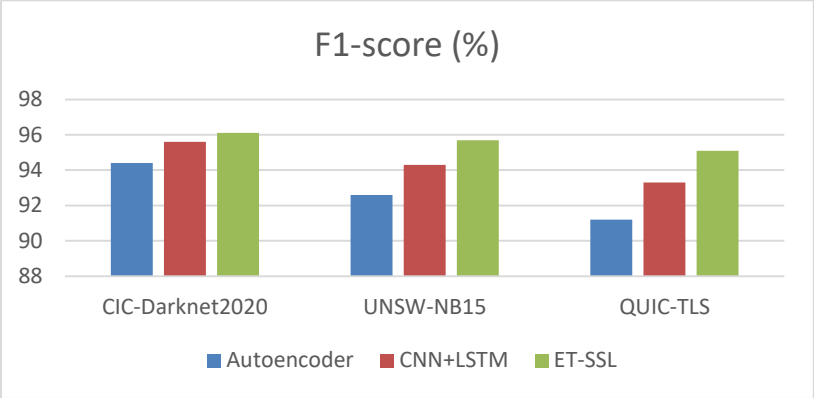

Fig. 2. F1 Score of Autoencoder, CNN+LSTM, and ET-SSL Models on Three Datasets

These indicators exceed the results of CNN+LSTM by 1–2 percentage points and significantly outperform the Autoencoder, which demonstrates F1 scores in the range of 0.912–0.944. This indicates the limited ability of the latter to adequately detect both positive and negative samples under encryption conditions [18, p. 46–48].

The third and highly important aspect is the false positive rate (FPR), which directly affects the operational value of the models. High FPR values lead to a large number of false alerts, potentially overloading the security analytics infrastructure and reducing trust in the system. Fig. 3 presents a comparison of FPR across all models.

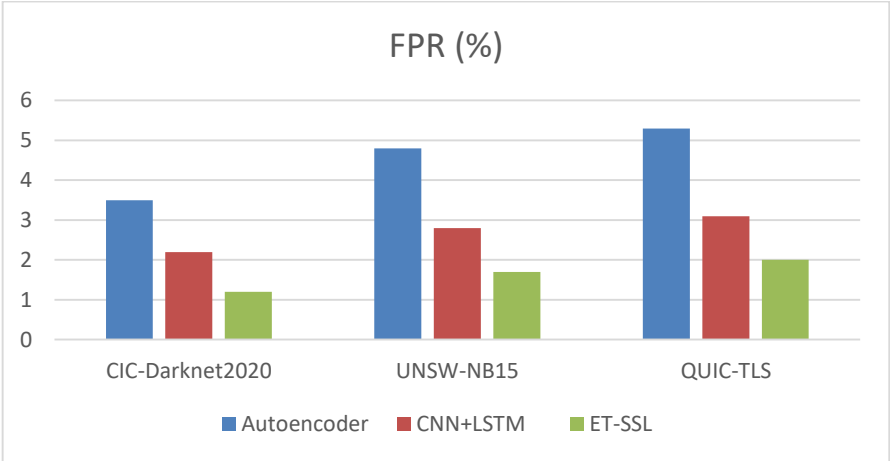

Fig. 3. False Positive Rate (FPR) of Autoencoder, CNN+LSTM, and ET-SSL Models

ET SSL once again demonstrates the lowest false positive rates: only 1.2% on CIC, 1.7% on UNSW, and 2.0% on QUIC-TLS. For comparison, CNN+LSTM falls within the 2.2–3.1% range, while the Autoencoder records critically high values — up to 5.3% on QUIC-TLS, making it virtually unsuitable for real-world deployment in a production environment.

INTERPRETATION OF RESULTS

The empirically validated results of anomaly detection in encrypted network traffic not only formalize the statistical success of the applied models but also provide a solid foundation for extrapolating their practical potential in real-world information and communication systems. The consistent classification accuracy exceeding 95% indicates the ability of modern

deep learning architectures to correctly differentiate network flows even without access to the content of transmitted packets — a fundamental limitation in the context of encryption.

Particular attention should be paid to the false positive rate (FPR), which is traditionally considered a critical parameter for real-time threat detection systems. In this regard, the ET SSL model demonstrates exceptionally low FPR values (<2% across all datasets), significantly reducing the risk of overloading alerting infrastructure and lowering the cognitive burden on human operators. Thus, the practical relevance of the ET SSL architecture in scalable environments is supported not only by its high accuracy but also by its efficiency in response resource utilization.

From an architectural innovation perspective, the ET SSL model, based on the concept of contrastive self-supervised learning, shows a remarkable ability to construct generalized latent spaces in which atypical samples can be heuristically distinguished. This approach does not rely heavily on prior data labeling, opening new opportunities for application in zero-day detection tasks — one of the most pressing challenges in modern cybersecurity. Therefore, the presented results justify interpreting the ET SSL model as a methodologically sound platform for developing adaptive, context-aware next-generation threat detection systems.

HYPERPARAMETER SENSITIVITY ANALYSIS

To assess the impact of key hyperparameters on model performance, a series of targeted experiments was conducted, focusing on variations in learning rate, time window size, and the Dropout regularization parameter. The analysis of the results made it possible to identify configurations that offer an optimal trade-off between classification accuracy, convergence speed, and computational complexity.

For the CNN+LSTM model, it was found that reducing the learning rate from 0.001 to 0.0005 improves classification accuracy by 0.8% (up to 97.5% on CIC-Darknet2020), although it also increases training time by approximately 40%. Further reduction of the learning rate below 0.0001 results in excessively slow convergence and a decline in the F1 score. Increasing the window size from 20 to 50 allows the model to capture longer temporal contexts, which positively impacts the F1 score (by up to +1.1%), though it also raises the resource intensity of processing. Meanwhile, increasing the Dropout rate from 0.3 to 0.5 leads to a decrease in accuracy (-0.8%), indicating loss of relevant information due to excessive regularization.

Table 2

Impact of Hyperparameters on CNN+LSTM Accuracy

Parameter	Value	Accuracy (%)
Learning rate	0.001	96.7
Learning rate	0.0005	97.5
Window size	20	96.7
Window size	50	97.8
Dropout	0.3	96.7
Dropout	0.5	95.9

Regarding the Autoencoder model, experiments revealed its sensitivity to architectural depth. Shallower configurations (64-32-16) offer faster training speeds but are less accurate (by 1.5–2%), whereas deeper architectures (256-128-64) yield higher performance but tend to overfit on smaller datasets. This necessitates the use of regularization techniques in combination with validated parameter selection methods such as grid search or Bayesian optimization.

Overall, the results of the hyperparameter sensitivity analysis confirm the importance of environment-specific adaptive tuning. Using static configurations without empirical validation may lead to inefficient resource usage or reduced threat detection performance in dynamic network conditions.

CONCLUSIONS AND FUTURE RESEARCH DIRECTIONS

As a result of the conducted study, it was established that modern deep learning-based approaches to anomaly detection in encrypted network traffic demonstrate high effectiveness even under conditions of limited access to the content of transmitted data. Among the tested models, the best performance was demonstrated by the ET SSL architecture, based on contrastive self-supervised learning mechanisms. It achieved the highest classification accuracy (up to 96.8%), F1 scores (up to 0.961), and the lowest false positive rate (as low as 1.2%).

The hyperparameter sensitivity analysis confirmed the importance of adaptive tuning of models to specific deployment environments. It was found that even small changes in window size, learning rate, or regularization level can significantly affect both classification accuracy and training convergence speed.

Thus, the results of this study support the feasibility of using deep neural networks for encrypted traffic threat detection without decryption, opening up new prospects for the development of next-generation intelligent cyber threat monitoring systems.

Future research directions include:

- Expanding the training base through new open datasets that cover modern encryption protocols (e.g., Encrypted SNI, DoQ, etc.);
- Integrating models into real-time IDS/IPS systems, ensuring scalability and low processing latency;
- Exploring explainable AI approaches to improve the transparency of model decision-making;
- Developing federated learning techniques to enhance privacy while maintaining model effectiveness in distributed networks;
- Adapting detection systems to adversarial attacks and developing defense mechanisms against them.

Overall, the obtained results can serve as a foundation for building adaptive, robust, and transparent threat detection systems suited for today's increasingly encrypted network environments.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Draper-Gil, G., Lashkari, A. H., Mamun, M. S. I., & Ghorbani, A. A. (2016). Characterization of encrypted and VPN traffic using time-related features. In *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)* (pp. 407–414). https://doi.org/10.5220/0005740704070414
2. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*. https://www.unb.ca/cic/datasets/ids-2017.html
3. Liu, Q., Zhang, Y., & Chen, T. (2023). DETD: A deep autoencoder-based anomaly detection framework for encrypted traffic. *Computational Intelligence and Neuroscience, 2023*, Article 3316642. https://doi.org/10.1155/2023/3316642

4. Wang, W., Zhu, M., Zeng, X., Ye, X., & Sheng, Y. (2018). HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection. *IEEE Access*, *6*, 1792–1806. https://doi.org/10.1109/ACCESS.2017.2780250
5. Fu, C., Li, Q., & Xu, K. (2023). HyperVision: Real-time encrypted traffic anomaly detection with contrastive learning. *arXiv preprint arXiv:2301.13686*. https://arxiv.org/abs/2301.13686
6. Sattar, S., Rehman, A., Khan, M., & Hussain, S. (2025). Anomaly detection in encrypted network traffic using self-supervised learning. *Scientific Reports*, *15*, Article 26585. https://www.nature.com/articles/s41598-025-08568-0
7. Canadian Institute for Cybersecurity. (2020). *CIC-Darknet2020 dataset*. https://www.unb.ca/cic/datasets/darknet2020.html
8. Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In *Military Communications and Information Systems Conference (MilCIS 2015)* (pp. 1–6). IEEE. https://doi.org/10.1109/MilCIS.2015.7348942
9. Aceto, G., Persico, V., & Pescapé, A. (2019). A survey on information and communication technologies for Industry 4.0: State-of-the-art, taxonomy, and open challenges. *Computer Networks*, *159*, 99–124. https://doi.org/10.1016/j.comnet.2019.05.010
10. Rokach, L., & Maimon, O. (2014). *Data mining with decision trees: Theory and applications* (2nd ed.). World Scientific Publishing. https://doi.org/10.1142/9097
11. Lotfollahi, M., Shirali Hossein Z., Jafari, S., & Saberian, M. (2020). Deep Packet: A novel approach for encrypted traffic classification using deep learning. *Soft Computing*, *24*, 1999–2012. https://doi.org/10.1007/s00500-019-04106-2
12. Lashkari, A. H., Draper-Gil, G., Mamun, M. S. I., & Ghorbani, A. A. (2017). Characterization of Tor traffic using time-based features. In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017)*. https://doi.org/10.5220/0006097702530260
13. Alsoufi, M., Liu, W., Khan, R., & Alazab, M. (2021). A survey of machine and deep learning methods for Internet of Things (IoT) security. *Sensors*, *21*(15), Article 5112. https://doi.org/10.3390/s21155112
14. Nanda, S., Zulkernine, M., & Haque, A. (2016). Predicting network attack patterns in encrypted traffic using machine learning. In *Proceedings of the IEEE International Conference on Big Data (Big Data)*. https://doi.org/10.1109/BigData.2016.7840625
15. Shbair, W., Zarpelão, B., & Granville, L. (2016). Efficient early detection of advanced persistent threats using network flow forensics. In *Proceedings of the 14th Annual Conference on Privacy, Security and Trust (PST)*. https://doi.org/10.1109/PST.2016.7906959
16. Lin, W., Xiao, X., Song, W., & Xue, Y. (2020). ID-RNN: An intrusion detection system based on a recurrent neural network. *Security and Communication Networks*, *2020*, Article 7690423. https://doi.org/10.1155/2020/7690423
17. Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cyber security. *Information*, *10*(4), Article 122. https://doi.org/10.3390/info10040122
18. Nguyen, T. T., & Armitage, G. (2008). A survey of techniques for Internet traffic classification using machine learning. *IEEE Communications Surveys & Tutorials*, *10*(4), 56–76. https://doi.org/10.1109/SURV.2008.080406

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

Підгорний Павло Володимирович
аспірант
Сумський державний університет, Суми, Україна
ORCID ID: 0009-0008-8604-8051
pashapro49@gmail.com

Лаврик Тетяна Володимирівна
кандидат педагогічних наук, доцент, старший викладач кафедри кібербезпеки
Сумський державний університет, Суми, Україна
ORCID ID:0000-0002-7144-7059
t.lavryk@dcs.sumdu.edu.ua

ВИЯВЛЕННЯ АНОМАЛІЙ У ЗАШИФРОВАНОМУ МЕРЕЖЕВОМУ ТРАФІКУ ЗА ДОПОМОГОЮ ГЛИБОКОГО НАВЧАННЯ

Анотація. Зростання частки зашифрованого трафіку в сучасних мережевих комунікаціях створює суттєві труднощі для кібербезпеки, особливо для традиційних систем виявлення вторгнень, що базуються на аналізі вмісту пакетів. У цьому дослідженні розглянуто проблему виявлення аномалій у зашифрованому мережевому трафіку за допомогою методів глибокого навчання, які аналізують метадані без необхідності розшифровування. Проведено комплексне експериментальне порівняння трьох архітектур — Autoencoder, CNN+LSTM та ET SSL (модель контрастного самоконтрольованого навчання) — з використанням трьох відкритих наборів даних: CIC-Darknet2020, UNSW-NB15 та QUIC-TLS, які охоплюють різноманітні типи зашифрованих протоколів і атак. Усі набори даних було попередньо оброблено до формату потоків (flows) із 75 стандартизованими числовими ознаками. Оцінка моделей виконувалася за точністю класифікації, F1-мірою та частотою хибнопозитивних спрацьовувань (FPR). Модель ET SSL показала найбільш стабільні та найкращі результати, досягнувши точності до 96,8%, F1-міри 0,961 та низького FPR — лише 1,2%. CNN+LSTM продемонструвала дещо нижчі, але конкурентні результати, тоді як модель Autoencoder виявила обмеження у здатності адаптуватися до високого рівня обфускації трафіку, особливо для потоків на основі протоколу QUIC. Крім того, було проведено аналіз чутливості гіперпараметрів, зокрема вивчався вплив швидкості навчання, розміру часового вікна та регуляризації dropout. Отримані результати підтвердили важливу роль адаптивного налаштування моделей для оптимізації їхньої продуктивності у конкретних умовах застосування. Наприклад, зменшення швидкості навчання покращувало точність, проте збільшувало час навчання, а подовження часового вікна покращувало F1-міру за рахунок підвищених обчислювальних витрат. Експериментальні результати підтверджують практичну доцільність застосування моделей глибокого навчання для моніторингу зашифрованого трафіку без необхідності його розшифровування. Особливо перспективною є архітектура ET SSL, що може бути використана у системах виявлення загроз у режимі реального часу завдяки своїй стійкості, високій здатності до узагальнення та низькій частоті хибнопозитивних результатів. Крім того, її здатність працювати в умовах обмеженої кількості розмічених даних або взагалі без них завдяки самоконтрольованому навчанню робить її особливо придатною для виявлення атак нульового дня. Майбутні напрямки досліджень включають розширення різноманітності навчальних наборів даних з урахуванням нових стандартів шифрування (наприклад, Encrypted SNI, DoQ), інтеграцію моделей у масштабовані середовища IDS/IPS з низькою затримкою, застосування методів пояснюваного штучного інтелекту (XAI) для підвищення довіри та прозорості, а також створення моделей, стійких до протидії супротивника. Представлені результати є основою для створення наступного покоління адаптивних і контекстно-орієнтованих систем моніторингу кіберзагроз.

Ключові слова: зашифрований трафік; виявлення аномалій; глибоке навчання; самоконтрольоване навчання; кібербезпека; ET SSL; CNN+LSTM; автокодер; QUIC; атаки «нульового дня».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Draper-Gil, G., Lashkari, A. H., Mamun, M. S. I., & Ghorbani, A. A. (2016). Characterization of encrypted and VPN traffic using time-related features. In *Proceedings of the 2nd International Conference on*

Information Systems Security and Privacy (ICISSP 2016) (pp. 407–414). https://doi.org/10.5220/0005740704070414

2. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*. https://www.unb.ca/cic/datasets/ids-2017.html
3. Liu, Q., Zhang, Y., & Chen, T. (2023). DETD: A deep autoencoder-based anomaly detection framework for encrypted traffic. *Computational Intelligence and Neuroscience*, *2023*, Article 3316642. https://doi.org/10.1155/2023/3316642
4. Wang, W., Zhu, M., Zeng, X., Ye, X., & Sheng, Y. (2018). HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection. *IEEE Access*, *6*, 1792–1806. https://doi.org/10.1109/ACCESS.2017.2780250
5. Fu, C., Li, Q., & Xu, K. (2023). HyperVision: Real-time encrypted traffic anomaly detection with contrastive learning. *arXiv preprint arXiv:2301.13686*. https://arxiv.org/abs/2301.13686
6. Sattar, S., Rehman, A., Khan, M., & Hussain, S. (2025). Anomaly detection in encrypted network traffic using self-supervised learning. *Scientific Reports*, *15*, Article 26585. https://www.nature.com/articles/s41598-025-08568-0
7. Canadian Institute for Cybersecurity. (2020). *CIC-Darknet2020 dataset*. https://www.unb.ca/cic/datasets/darknet2020.html
8. Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In *Military Communications and Information Systems Conference (MilCIS 2015)* (pp. 1–6). IEEE. https://doi.org/10.1109/MilCIS.2015.7348942
9. Aceto, G., Persico, V., & Pescapé, A. (2019). A survey on information and communication technologies for Industry 4.0: State-of-the-art, taxonomy, and open challenges. *Computer Networks*, *159*, 99–124. https://doi.org/10.1016/j.comnet.2019.05.010
10. Rokach, L., & Maimon, O. (2014). *Data mining with decision trees: Theory and applications* (2nd ed.). World Scientific Publishing. https://doi.org/10.1142/9097
11. Lotfollahi, M., Shirali Hossein Z., Jafari, S., & Saberian, M. (2020). Deep Packet: A novel approach for encrypted traffic classification using deep learning. *Soft Computing*, *24*, 1999–2012. https://doi.org/10.1007/s00500-019-04106-2
12. Lashkari, A. H., Draper-Gil, G., Mamun, M. S. I., & Ghorbani, A. A. (2017). Characterization of Tor traffic using time-based features. In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017)*. https://doi.org/10.5220/0006097702530260
13. Alsoufi, M., Liu, W., Khan, R., & Alazab, M. (2021). A survey of machine and deep learning methods for Internet of Things (IoT) security. *Sensors*, *21*(15), Article 5112. https://doi.org/10.3390/s21155112
14. Nanda, S., Zulkernine, M., & Haque, A. (2016). Predicting network attack patterns in encrypted traffic using machine learning. In *Proceedings of the IEEE International Conference on Big Data (Big Data)*. https://doi.org/10.1109/BigData.2016.7840625
15. Shbair, W., Zarpelão, B., & Granville, L. (2016). Efficient early detection of advanced persistent threats using network flow forensics. In *Proceedings of the 14th Annual Conference on Privacy, Security and Trust (PST)*. https://doi.org/10.1109/PST.2016.7906959
16. Lin, W., Xiao, X., Song, W., & Xue, Y. (2020). ID-RNN: An intrusion detection system based on a recurrent neural network. *Security and Communication Networks*, *2020*, Article 7690423. https://doi.org/10.1155/2020/7690423
17. Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cyber security. *Information*, *10*(4), Article 122. https://doi.org/10.3390/info10040122
18. Nguyen, T. T., & Armitage, G. (2008). A survey of techniques for Internet traffic classification using machine learning. *IEEE Communications Surveys & Tutorials*, *10*(4), 56–76. https://doi.org/10.1109/SURV.2008.080406