A Comparative Study of Machine Learning and Deep Learning Methods in Anomaly Detection for Expanding Network Infrastructures

[1]Nyarkisa Christopher Sebit Elias ,[2]Diko Francis Michael Peter, [3]Omkar Pattnaik, [4]Laureen Kalakaw George, [5]Luany Yiek Juor

[1,2,4,5] Student, School of Computer Science and Engineering, Sandip University, Nashik, Maharashtra-422213, India

[3]Associate Professor, School of Computer Science and Engineering, Sandip University, Nashik, Maharashtra-422213, India

Abstract-With the increased infrastructure in IoT device networks and SDN and the necessity of the security and trustworthiness of these networks to increase, there is mounting demand for smart network traffic analysis and anomaly detection. Machine learning (ML) and deep learning are prominent components in studies in the context of anomaly detection and botnet prevention. Wong and Arjunan demonstrated scalability's importance through creating a model of deep learning-based anomaly detection for big-scale data environments. Liu and Park also illustrated the possibility of reinforcing anonymous traffic detection accuracy, and Shoman and Wang proposed a model of video captioning for intelligent transportation surveillance, in real-time. Ghamri-Douden presented a visual method for identifying botnet activity in IoT technologies, and Arnold and Gromov proposed a CNN solution for detecting botnets in IoT to reduce the vulnerabilities of IoT. These studies illustrate the importance of AI-based techniques for the quick identification of botnet attacks.

Keywords: Supervision training, Neural Networks, Intrusion Detection Systems (IDS)

1.INTRODUCTION

As the world becomes increasingly networked, monitoring and securing facilities like Cloud infrastructure, SDN, and the Internet of Things requires monitoring and inspection of network traffic as well as potentially anomaly detection. [11] Sophisticated Traffic analysis techniques now face new challenges owing to the rampant proliferation of networked devices and information, which demands increased focus on timely and effective anomaly detection for improved security and reliability. Classical network security approaches fail because of the dynamic and heterogeneous nature of the data, which necessitates the deployment of machine learning (ML) [2,5] and deep learning (DL) techniques in real time.

Figure: Anomalies Detection

Wong and Arjunan (2023) [2] designed a 'big data' deep learning model for anomaly detection, while Shoman and Wang (2023) [1] discussed the requirement for high-speed and scalable big data processing in real-time traffic safety smart transport systems with the use of video captioning [3, 5]. Liu and Park (2023) [3] presented a feature engineered reinforcement learning (RL) approach toward traffic classification for the issues faced in recognizing unexpected traffic movements. Besides, as shown by Arnold and Gromov (2023), who employed CNNs and traffic visualization for IoT botnet detection, and Korba et al. (2023) [11], who suggested an AI-driven early detection approach, IoT networks are highly susceptible to botnets. A terabit-speed monitoring framework based on AI, MARINA, was presented by Seufert et al. (2023) for real-time performance and security issue detection. Network traffic analysis for malware and ransomware detection is also essential. While Rana et al. (2023) [16] aimed at malware detection using behavioural analysis, Mehrban and Geransayeh (2023) [9] presented an ML-based ransomware detection model from traffic behaviour. Pillai and Polimetla (2023) [17] address privacy concerns in network monitoring through a privacy-preserving framework with homomorphic encryption to enable secure traffic analysis without losing sensitive data.

2.LITERATURE REVIEW

Intelligent transportation systems (ITS) increasingly utilize real-time video analysis for traffic safety, e.g., in Shoman and Wang's (2023) [1] dense video captioning model, which records and describes multiple road events simultaneously to improve incident detection accuracy in heavy traffic zones. In large data settings, Wong and Arjunan (2023) [2] developed a deep learning model for real-time anomaly detection, ideal for high-traffic networks where rapid responses are crucial to prevent failures. Tamilselvan Arjunan further explores ML integration to boost detection speed and accuracy. Liu and Park (2023) [3] addressed the challenge of identifying anonymous traffic by creating a reinforcement learning system with feature engineering, allowing dynamic adaptation to traffic changes. For botnet-attack-vulnerable IoT networks, Arnold and Gromov (2023) [4] proposed a CNN model displaying traffic behaviour, improving detection through the detection of botnet signatures, while Korba et al. (2023) [11] proposed an AI-powered early botnet detection mechanism for avoiding attack effects. Seufert et al. (2023) [5] offered MARINA, an ML-driven framework for terabit-scale traffic monitoring, with real-time efficiency in anomaly detection for 5G networks and data centres. Zhukabayewa et al. (2023) [14] proposed in smart grids a traffic analysis framework via ML-based node classification for enhanced cyber threat detection in WANs essential for energy distribution networks. Malware and ransomware identification in network traffic is fast emerging as the critical requirement, given that cybercriminals increasingly use sophisticated mechanisms to evade detection.

Mehrban and Geransayeh (2023) [9] also developed an ML-based model to identify ransomware based on network traffic behaviour analysis in order to facilitate quick response. Similarly, Rana et al. (2023) [16] employed ML to detect malware based on behavioural characteristics rather than traditional signatures, facilitating resilience against diverse threats. Network traffic analysis privacy concerns are tackled by Pillai and Polimetla (2023) [17] employing homomorphic encryption that enables the analysis of encrypted data without compromising security in addition to data privacy.

Another standout focus area includes maximizing traffic analysis pipelines; Wan et al. (2023) [8] introduced the CATO framework for efficient ML-based traffic analysis, and Wang and Qian (2023) [10] developed Lens, a scalable model that is adaptable across diverse networks for real-time observation.

Some of the new techniques in malicious traffic detection include ContraMTD by Han et al. (2023) [15], a contrastive learning-based method effective with scarce labelled data, and Gioacchini et al. (2023) [12], who utilized multi-model representation learning for boosting detection accuracy and scalability for security-critical network

3.METHODOLOGY COMPARISON AND EVALUATIONS

Real-Time Anomaly Detection in Big Data, High-Throughput Environments

Real-time anomaly detection is essential in big data, high-throughput environments. Wong and Arjunan (2023), Ness S, Sridharan and Shinde (2025) [2&22] developed a deep learning model optimized for fast detection in large volumes of data with high scalability and accuracy but with the price of large computational resources. Tamilselvan Arjunan (2023) [19] further enhanced this model with latency-reducing optimizations. Seufert et al. (2023) [5] introduced MARINA, a terabit-scale traffic analysis system for data canters and 5G networks, which is optimally designed for high-speed anomaly detection. Wong and Arjunan's model, in general, fits well in resource-scarce environments compared to MARINA in resource-abundant environments.

Detection of Encrypted or Anonymous Traffic

The growth in anonymous and encrypted traffic is a challenge to the traditional detection methods reliant on observable patterns of data. Liu and Park (2023) [7] overcome this by combining feature engineering with reinforcement learning, which allows their model to detect anonymous traffic based on contextual pattern detection rather than actual identifiers.

Assessment: Liu and Park's model is extremely efficient in the detection of anonymous traffic, especially where the traditional strong point, despite the necessity of feature engineering which may hinder having extensive usage, lies.

IoT Botnet Detection and Visualization Techniques

Vulnerable IoT networks are the target point for research into botnet detection. Arnold and Gromov (2023), Kontagora, M. M., Adeshina, S. A., & Musa H. (2025) [4&23] employ convolutional neural networks (CNNs) with traffic visualization, converting network patterns into visual signatures that CNNs recognize, with high accuracy in IoT botnet detection. However, the scalability of the approach may be limited in mixed-traffic networks. Korba et al. (2023) [11] extend this by developing an AI-based rapid-response mechanism for early botnet detection, enabling proactive defences.

Evaluation: Arnold and Gromov's strategy are ideal for IoT networks, but Korba et al.'s rapid-response model is ideal for networks demanding real-time detection and reactive defences.

Privacy-Conscious Traffic Analysis

As more concern is raised over data privacy, studies have shifted their interests to privacy-protected network traffic monitoring. Pillai and Polimetla (2023) [17] employ homomorphic encryption, which allows processing of encrypted data for the purpose of protecting sensitive information, and hence is suitable for controlled sectors like healthcare and finance.

Evaluation: Pillai and Polymedia’s approach is very effective in privacy-sensitive environments, though the requirement for processing results in it not being as good for situations involving the need to do quick real-time analysis.

Ransomware and Malware Detection through Network Traffic Analysis

Malware detection by network traffic patterns and ransomware is critical to cybersecurity. Mehrban and Geransayeh (2023) [9] use machine learning to identify ransomware based on behaviour, but zero-day instances may get past. Similarly, Rana et al. (2023) [9] & [16] are focused on malware detection using classification of perilous traffic based on behaviour rather than static signatures, which is more flexible but relies on labelled data, restricting its flexibility to novel malware.

Assessment: Both models improve threat detection over signature-based systems but are ineffective against zero-day attacks and must be updated frequently to be useful.

Large Data Streams Monitoring Frameworks in Real-Time

For large-scale data environments, frameworks like CATO and Lens streamline traffic analysis efficiency. Wan et al. (2023) [8] introduce CATO, a combined machine learning system for traffic analysis that offers increased processing efficiency and usage in huge networks but may require customization for different configurations such as hometown networks, city networks, and phone networks. Lens, which Wang and Qian (2023) [10] designed, offers a generalized framework versatile across multiple types of networks but with a broad approach at the potential cost of accuracy to specialized models.

Evaluation: Both models are good for large-scale networks, with CATO being very efficient and Lens being very flexible. CATO does, however, need to be adapted for specific networks, whereas Lens sacrifices some precision for generality.

Contrastive and Representation Learning for Malicious Traffic Detection

Increasing contrastive learning methods are performing satisfactorily for unsupervised detection. Han et al. (2023) [15] introduce ContraMTD, an unsupervised model, based on contrastive learning to detect benign vs. malicious traffic behaviour by minimizing labeled data and being efficient for detection of unknown threats Gioacchini et al. (2023) [12] report a multi-model representation learning method that enhances traffic analysis by combining several models to increase the precision of anomaly detection in complex network settings.

Evaluation: Both methods significantly contribute to the discovery of unknown and evolving threats. ContraMTD does well in situations with little labelled data, while the multi-model method offers sufficient accuracy but could be resource-intensive and therefore suitable for high-capacity network.

4.CHALLENGES/PROBLEMS AND SOLUTIONS

s/no	Research topics	Challenges/problems	Solutions

01	Generic Multi-Modal Representation Learning for Network Traffic Analysis.	Traditional methods are generally bogged down by the complexity and dynamic nature of traffic scenarios, where it difficult to generate accurate and comprehensive captions.	The paper presents a dense captioning framework based on parallel decoding for video captioning and CLIP visual features. The end-to-end model adds to dense captioning in the context of traffic safety videos, particularly pedestrians versus vehicle. With such methodologies integrated, the framework is capable of better visual-language sequences and generating informative captions for video inspection.
02	Real-Time Detection of Network Traffic Anomalies in Big Data Environments Using Deep Learning Mode.	Traditional methods generally are bogged down by the amount and velocity of data, where it is difficult to pinpoint anomalies in a timely and accurate fashion.	The paper proposes a framework of deep learning using convolutional neutral networks and long short-term memory models. The combination allows for effective real-time detection through the synergy of the capabilities of CNNs (for spatial feature extraction) and LSTMs (for temporal feature analysis.
03	Marina: Realizing ML – Driven Real- Time Network Traffic Monitoring at Terabit Scale.	Legacy monitoring system tend to struggle with the enormous us rates of data and provide real-time analysis.	The paper introduces Marina, which combines a very efficient data plane to sample traffic statistics at line with a efficient ML server for running demanding monitoring inference models. It allows for real-time and scalable network traffic observation at terabit scale by utilizing machine learning for efficiently handling high data rates.
04	Descriptive Analysis of wide area network flow control internet traffic on Metro-E 100 Mbps campus network.	Issue of network congestion and QoS delays on a campus network. As the traffic on the internet grows, it can contribute to spikes of networks capacity, impacting network performance overall.	The article provides a descriptive analysis to enhance bandwidth management within the metro E network. According to the flow control internet traffic analysis the study provides results and suggestions for enhancing network performance and managing congestion more effectively.
05	IoT network traffic analysis using deep learning.	The issue of networks congestion and Quality of service delays in a campus network. With growth in the internet traffic it can create bursts of network capacity impacting overall network performance. The problem of anomaly detection and monitoring in loT network traffic. Because loT networks are becoming complex and producing enormous amount of dynamic data statistical approaches and machine learning based methods are unable to monitor and detect anomalies effectively.	The paper proposes applying deep learning techniques to analyse loT networks traffic.in particular they used an ensemble-based model on the KDD cup 99 dataset which was found to ne very high in performance having an accuracy rate od over 98% the technique allows for more efficient in loT network.
06	Cato: end to end optimization of ML-based traffic analysis pipeline.	CATO; end to end optimization if ML-based traffic analysis pipelines addresses the problem of efficiently deploying machine learning models or network traffic analysis even though ML models have a great potential to improve traffic analysis, it is difficult to deploy them in real life because	The article introduces CATO a model that uses multi-objective Bayesian optimization to search for pareto-configuration. The makes it possible for CATO to automatically construct end to end optimized serving pipelines to be deployed directly in real networks

		they need the two to be balanced, i.e., system costs and model's performance.	effectively decreasing system costs with maximum model performance.
07	Anomalous traffic detection system in SDN via hybrid deep learning models.	Problem of detecting abnormal traffic in software defined networking (SDN) environments in traditional methods of abnormal.	The proposes a hierarchic AI detection scheme that incorporates port information and wavelet transform for coarse detection, and deep learning the techniques for fine detection and deep learning techniques for fine detection 3. This fusion approach possesses overall advantages for rapid and precise abnormal detection, thus improving network security and performance.
08	AI-Powered Fast and Early IoT Botnet Detection.	Problem of capturing stealth bot communication that coordinates attack in IoT networks1. In the past, traditional approaches don't detect them early-stage communications, the possibility of serious security breaches.	The paper prescribes an end -to-end approach to IOT network traffic analysis considering both bidirectional and unidirectional flows and packet formats 2, Using AI and machine learning techniques, the paper demonstrates the feasibility of early botnets traffic detection, with special emphasis on stealth command and control (c2) communications.
09	Generic Multi-Modal Representation Learning for Network Traffic Analysis.	Problem of creating custom deep learning architectures for each and every single network traffic analysis task. Traditional methods are often based on customised solutions, which can be time consuming and not very efficient.	The paper proposes an adaptive multi-model Autoencoder (MAE) pipeline on top of generic data adaptation modules to handle different types of network traffic measurement 1. The modules are integrated into a compact and expressive intermediate representation (i.e. embeddings) allowing the traffic analysis tasks without custom architectures.
10	ContraMTD: an UNSURPERVISED Malicious Network Traffic Detection Method based on Contrastive.	Problem of detecting malicious network traffic without relying on labelled data. Traditional methods are often based on labelled datasets, which can be difficult and expensive to obtain.	The work introduces ContraMTD, a novel method combining graph neural network with contractive learning to detect malicious traffic it projects local behaviour features and global interaction features from normal network traffic and then utilizes contrastive learning to obtain consistency between such features. this allow ContraMTD to ineffectively detect anomalies that deviate from pre-learned patterns supporting unsupervised detection of malicious traffic.

5. CONCLUSION

In conclusion, the field of network traffic analysis is evolving rapidly due to advancements in AI and ML technologies, necessitating a focus on improving detection capabilities against sophisticated cyber threats while addressing privacy concerns. Future research should prioritize the development of hybrid models and self-learning algorithms, alongside robust privacy-preserving techniques like federated learning and secure multi-party computation. The challenges presented by IoT environments call for lightweight detection algorithms and edge computing solutions to support real-time monitoring. As network data volumes increase, scalable solutions such as distributed architectures and stream processing frameworks will be crucial.

6.FUTURE SCOPES

Some future work directions for the discussed subjects are:

1. Generic Multi-Modal Representation Learning for Network Traffic Analysis

Use the dense captioning model to analyse other dynamic scenes apart from traffic safety, such as monitoring in smart cities or disaster response.

Explore the use of 3D video data with LiDAR features for more diversified captioning in traffic tasks.

Explore using reinforcement learning to optimize additional visual-language sequence generation.

2. Real-Time Network Traffic Anomaly Detection in Big Data Scenarios Using Deep Learning Models

Combine hybrid models with CNNs, LSTMs, and transformer models to perform better on larger datasets.

Design anomaly-detection frameworks that are edge-computing compatible for low-latency applications.

Address concept drift issues in dynamic big data scenarios using online learning methods.

3. Marina: Scaling ML-Powered Real-Time Network Traffic Monitoring to Terabit Scale

Marina to include predictive analytics to forecast traffic congestion and anomalies.

Investigate energy-efficient methods to ML model inference to reduce operational cost at terabit scale.

Include multi-modal data fusion for better insight into network traffic behavior.

4. Descriptive Analysis of Wide Area Network Flow Control Internet Traffic on Metro-E 100 Mbps Campus Network

Apply real-time flow control mechanisms based on machine learning to predict and counter congestion spikes.

Develop adaptive bandwidth allocation schedules based on historical traffic patterns and real-time consumption.

Explore cross-layer optimization techniques to further enhance Quality of Service (QoS).

5. Deep Learning for IoT Network Traffic Analysis

Extend the ensemble-based methodology to process real-time IoT data streams towards dynamic and instant responses to threats.

Utilize federated learning techniques for privacy-preserving IoT traffic analysis in distributed environments.

Examine context-aware anomaly detection frameworks that can dynamically adapt to diverse IoT application environments.

6. CATO: End-to-End Optimization of ML-Based Traffic Analysis Pipelines

Explore the use of integrating CATO with AutoML frameworks to broaden its range of applications.

Investigate the use of quantum computing to facilitate quicker optimization for more complex ML pipelines.

Develop adaptive optimization methods for real-time network setup and cost-performance trade-offs.

7. SDN Anomalous Traffic Detection System through Hybrid Deep Learning Models

Integrate hybrid deep learning models with network segmentation mechanisms to enhance anomaly isolation.

Integrate self-healing mechanisms into the SDN traffic detection system to automatically remove detected faults.

Explore the integration of blockchain-based audit trails for greater security and traceability.

8. AI-Aided Quick and Early IoT Botnet Detection

Develop cross-protocol detection mechanisms to identify botnet communication between different IoT devices.

Include adversarial training to make detection models resistant to evasive techniques.

Investigate transfer learning methods for rapid adaptation of detection models against new botnet variants.

9. Generic Multi-Modal Representation Learning for Network Traffic Analysis (Autoencoder Pipeline)

Update the adaptive multi-model autoencoder pipeline using self-supervised learning approaches to reduce reliance on labelled data.

Use lightweight variants of the pipeline to enable deployment on resource-limited platforms like edge devices.

Expand the applicability to emerging network paradigms, for instance, satellite networking or 6G networks.

10. ContraMTD: Unsupervised Malicious Network Traffic Detection using Contrastive Learning

Generalize ContraMTD to include cross-domain learning for better generalization across different network scenarios.

Design real-time functionality to enable proactive malicious traffic identification.

Integrate the framework with federated learning to enhance scalability and privacy in decentralized settings.

These directions are promising opportunities to overcome existing limitations while extending the scope of suggested methodologies!

REFERENCES

[1] Shoman, M., & Wang, D. (2023). Enhancing traffic safety with parallel dense video captioning for end-to-end event analysis. Smart and Safe Transportation (SST) Lab, University of Central Florida.

[2] Wong, M. L., & Arjunan, T. (2023). Real-time detection of network traffic anomalies in big data environments using deep learning models. International Journal of Big Data Intelligence, 9(1), 14-22.

[3] Liu, D., & Park, Y. (2023). Anonymous traffic detection based on feature engineering and reinforcement learning. Charles W. Davidson College of Engineering, San Jose State University.

[4] Arnold, D., & Gromov, M. (2023). Network traffic visualization coupled with convolutional neural networks for better IoT botnet detection. IEEE Internet of Things Journal, 10(4), 2392-2405.

[5] Seufert, M., Dietz, K., Webner, N., Geibler, S., Schuler, J., Wolz, M., Hotho, A., Casas, P., Hobfeld, T., & Feldmann, A. (2023). Marina: Realizing ML-driven real-time network traffic monitoring at terabit scale. IEEE Transactions on Network and Service Management, 20(2), 1234-1248.

[6] Wang, K., Fu, Y., Duan, X., Liu, T., & Xu, J. (2023). Abnormal traffic detection system in SDN based on deep learning hybrid models. IEEE Access, 11, 111-123.

[7] Liu, M., & Yang, L. (2023). IoT network traffic analysis with deep learning. International Journal of Network Management, 32(4), e2212.

[8] Wan, G., Liu, S., Bronzino, F., Feamster, N., & Durumeric, Z. (2023). CATO: End-to-end optimization of ML-based traffic analysis pipelines. Stanford University, University of Chicago, Ecole Normale Supérieure de Lyon.

[9] Mehrban, A., & Geransayeh, S. K. (2023). Ransomware threat mitigation using network traffic analysis and machine learning methods. Journal of Cyber Security Technology, 7(2), 89-100.

[10] Wang, Q., & Qian, C. (2023). Lens: A foundation model for network traffic. IEEE Transactions on Network and Service Management, 20(1), 245-259.

[11] Amara, A., Korba, A., Dial, A., & Ghamri-Duodane, Y. (2023). AI-driven fast and early detection of IoT botnet threats: A comprehensive network traffic analysis approach. LRS, Badji Mokhtar University of Annaba, Algeria.

[12] Gioacchini, L., Mellia, M., Drago, I., & Rossi, D. (2023). Generic multi-model representation learning for network traffic analysis. IEEE Transactions on Network and Service Management, 20(1), 1-15.

[13] Paezah, N., Kassin, M., Mohd Deni, S., & Mohd Yussof, Y. (2023). Descriptive analysis of wide area network flow control internet traffic on metro-E 100 Mbps campus network. International Journal of Electrical Engineering Education, 60(1), 32-40.

[14] Zhukabayewa, T., Pervez, A., & Mardenov, Y. (2023). A traffic analysis and node categorization-aware machine learning-integrated framework for cybersecurity intrusion detection and prevention of WSNs in smart grids. International Journal of Network Security, 25(2), 123-135.

[15] Han, X., Cui, S., & Qin, J. (2023). ContraMTD: An unsupervised malicious network traffic detection method based on contrastive learning. IEEE Transactions on Information Forensics and Security, 18(2), 678-690.

[16] Rana, K., Gupta, S., & Kaur, G. (2023). Malware detection in network traffic using machine learning. International Journal of Computer Applications, 182(9), 30-36.

[17] Vadakkethil, S. E., Pillai, S., & Polimetla, K. (2023). Privacy-preserving network traffic analysis using homomorphic encryption. Journal of Electrical Engineering & Computer Sciences, 8(1), 55-70.

[18] Dhumane, A., Sakhtare, N. N., & Deharkar, P. (2023). Design of an efficient forensic layer for IoT network traffic analysis engine using deep packet inspection via recurrent neural networks. Journal of Computer Science and Engineering, 12(3), 145-158.

[19] Arjunan, T. (2023). Real-time detection of network traffic anomalies in big data environments using deep learning models. Journal of Data Science and Analytics, 15(3), 210-220.

[20] Saleem, J., Islam, R., & Islam, M. Z. (2023). Darknet traffic analysis: A systematic literature review.

[21] Journal of Computing and Security, 14(2), 101-115.

[22] Ness, S., Eswarakrishnan, V., Sridharan, H., Shinde, V., Janapareddy, N. V. P., & Dhanawat, V. (2025). Anomaly detection in network traffic using advanced machine learning techniques.

[23] Chen, Y., & Zhang, L. (2023). Federated learning for privacy-preserving network traffic classification. IEEE Access, 11, 21543–21556.

[24] Bashir, S., & Wani, M. A. (2023). Adaptive anomaly detection in cloud traffic using generative adversarial networks. International Journal of Cloud Applications and Computing, 13(1), 54–67.

[25] Kim, J., & Shin, H. (2023). FlowGAN: Leveraging GANs for synthetic network traffic generation and anomaly detection. IEEE Transactions on Dependable and Secure Computing, 20(3), 782–794.

[26] Patel, R., & Shah, N. (2023). Deep ensemble learning for encrypted traffic classification. Journal of Cybersecurity and Information Management, 9(2), 134–147.

[27] Romero, M., & Garcia, D. (2023). Explainable AI for intrusion detection in network traffic: A SHAP-based approach. Journal of Network and Computer Applications, 215, 103572.

[28] Otieno, S., & Kariuki, P. (2023). Detection of stealthy DDoS attacks using hybrid deep learning models. Journal of Information Security Research, 11(4), 201–213.

[29] Tiwari, R., & Mehta, A. (2023). Lightweight machine learning model for IoT edge traffic classification. Future Internet, 15(2), 45–59.

[30] Nasiri, M., & Ahmadi, H. (2023). Time-series prediction of abnormal network behavior using LSTM and attention mechanisms. Journal of Big Data Analytics in Cybersecurity, 6(1), 24–38.

[31] De Silva, R., & Perera, S. (2023). A comparative study on supervised vs unsupervised ML algorithms for encrypted traffic analysis. IEEE Communications Surveys & Tutorials, 25(1), 65–84.

[32] Qureshi, A., & Malik, F. (2023). Enhancing SDN security with real-time traffic inspection and CNN models. IEEE Transactions on Network and Service Management, 20(3), 1780–1792.

[33] Mohanty, A., & Jena, R. (2023). Transfer learning-based detection of zero-day attacks in network traffic. Journal of Intelligent & Fuzzy Systems, 44(6), 7329–7341.

[34] Zaman, T., & Basharat, A. (2023). Towards resilient network security: A reinforcement learning-based adaptive IDS. International Journal of Security and Networks, 18(2), 101–116.

[35] Ahmed, H., & Ibrahim, M. (2023). Correlation-aware multi-feature traffic analysis for botnet detection. Journal of Cyber-Physical Systems, 7(3), 193–208.

[36] Du, Y., & Chen, M. (2023). Real-time anomaly prediction in 5G networks using bidirectional GRUs. IEEE Transactions on Mobile Computing, 22(1), 440–451.

[37] Singh, P., & Rajan, A. (2023). DeepGraphIDS: Graph neural networks for network intrusion detection. Computer Networks, 226, 109709.