International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 12, pp 11-19, December-2024

https://doi.org/10.47001/IRJIET/2024.812002

Survey of Computer Network Traffic Analysis Using Artificial Intelligence Algorithms

[1]*Osama Yassin Mohammed, [2]Ibrahim Ahmed Saleh

[1]Student, Department of Computer Science, College of Computer & Math., University of Mosul, Iraq

[2]Professor, Department of Software, College of Computer & Math., University of Mosul, Iraq

***Abstract* - This paper introduces a literature review and experimental scenario for network construction; the paper analyzes the network traffic analysis status with artificial intelligence algorithms such as machine learning (ML), ensemble learning, and deep learning for study about analysis in traffic, cybersecurity, balanced loading of network and prediction the traffic moving. The technical aspects of AI are used to analyze and detect attacks or conjunctions for large amounts of network data, thereby detecting anomalies or malicious activities that affect networks. Also, when training deep learning such as convolution neural networks (CNN) or recurrent neural networks (RNN) for datasets (historical data), learn benign network behavior as well as anomalies that may result from malicious activities. The paper introduces how AI technology is used to detect security threats and analyze networks on an outstanding basis.**

Keywords: Network Analysis, Intelligence Algorithms, Network Security, Anomaly Detection, Cyber Threat Detection.

I. INTRODUCTION

With the increasing importance of network and the increasing complexity of network structures, it is increasingly necessary to have an in-depth understanding and analysis of the overall network topology and network behavior in order to find network bottlenecks, optimize network configuration, and further discover potential dangers that may exist in the network. To this end, it is necessary to dynamically describe large-scale network structures and analyze network performance based on changes in network traffic, providing a technical platform for strengthening network management, improving network utilization, and preventing large-scale network attacks. The measurement and analysis of network has become one of important issues of general concern to academia, business, and national government departments [1]. The emergence of a new era based on linking more than one component to a network has led to rising requirements and the imposition of new challenges on those responsible for managing this connection.

The most important of these challenges is maintaining the integrity of data across the network and the privacy of beneficiaries of the services provided by the network, which can be achieved through optimal management of resources, the continuity of providing the service, and possibility of access to obtain the highest level of customer satisfaction. From this standpoint, studying and analyzing the behavior generated by the traffic resulting from the activity of individuals connected to the network has become an essential component to ensure the achievement of the concept of cyber security. Traffic analysis depends on methods of reading and collecting network data. Then, the method used to analyze it, whether statistically or using more advanced techniques such as artificial intelligence technologies. All this effort is to ensure the enhancement of the security of the network and raise its performance [1].

AI plays a pivotal role in improving network traffic analysis, which significantly improves both security and efficiency. By leveraging various AI technologies, organizations can improve network performance, detect malicious activity, and manage traffic more effectively. The following sections describe the critical applications of AI in this area. Organizations recognize the influential role of AI technologies in supporting network traffic analysis methods to improve overall network performance and detect malicious activity, which improves both security and efficiency. Effective analysis of AI algorithms such as machine learning and deep learning enables proactive adjustments to network configuration, and reinforcement learning techniques can improve routing and resource allocation and enhance overall network efficiency [2], [3]. AI plays a pivotal role in improving network traffic analysis, which significantly improves both security and efficiency. By leveraging various AI technologies, organizations can improve network performance, detect malicious activity, and manage traffic more effectively. The following sections describe the critical applications of AI in this area. Organizations recognize the influential role of AI technologies in supporting network traffic analysis methods to improve overall network performance and detect malicious activity, which improves both security and efficiency. Effective analysis of AI algorithms such as machine learning and deep learning

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 12, pp 11-19, December-2024

https://doi.org/10.47001/IRJIET/2024.812002

enables proactive adjustments to network configuration, and reinforcement learning techniques can improve routing and resource allocation and enhance overall network efficiency [2], [3].

II. NETWORK TRAFFIC ANALYSIS

Network Traffic Analysis (NTA) is the process of observing network data traffic over a period of time to ensure efficient and secure operations while also tracking normal traffic patterns and identifying unusual behavior. NTA involves collecting, inspecting, evaluating, and understanding the information packets running on a network. With the complexity of networks continuing to grow and with the reliance users place on services running over this infrastructure, the importance of NTA as a tool for managing network performance also increases. With the increase in threats to organizational network infrastructure, whether from insiders or from cyber predators, the importance placed on NTA also greatly increases. [1], [4].

NTA reduces issue identification time. It saves costs by detecting network performance issues before other tools. NTA provides real-time and long-term traffic analysis. Signatures are needed for pattern detection. Traffic analyses tools help diagnose network problems. Users need training on software to respond to events. Supported protocols include Cisco NetFlow, Juniper JFLOW, and Flow. NTA offers trend analysis over time. It aids in low-level performance analysis. This paper covers NTA requirements for data mining algorithms to generate valuable information for organizations.

Network traffic analysis is a procedure by which network behavior can be observed, analyzed, and determined based on the available data [5]. There are three major network traffic analysis techniques, each of which provides its own insights into network behavior. The most fundamental of these techniques is packet inspection, an approach that involves examining packet contents. A second technique, flow analysis, involves examining flows happening within the network. Flows are collections of packets over a certain time period being transmitted between source and destination. Various flow analysis techniques primarily focus on generating descriptive statistics and identifying patterns and asymmetries in the flow of payloads [1], [6]. In some cases, classification or identification is necessary. The procedures by which application-layer protocols are detected are collectively referred to as protocol identification. Various methods of identifying protocols exist, with differing levels of sophistication. However, understanding how data packets are remotely transmitted and communicated can provide actionable information about a network [7], [8]. Understanding the packet inspection process is essential in analyzing traffic, enhancing the quality, comprehensiveness, and visual impact of network reporting. Connecting these techniques into one solution is crucial.

III. RESULTS AND DISCUSSIONS

There are many researchers concluded that papers with analysis of network achieved better performance, summarize some of important of them.

In 2024, Farzaan *et al.* [9] proposed in their paper an AI-powered cyber incident response system for cloud environments to address increasing cyber threats. Tested on three datasets (NSL-KDD, UNSW-NB15, CIC-IDS-2017), the system achieved high accuracy using Random Forest (up to 99%) and neural networks (99% for malware analysis). It integrates seamlessly with platforms like Google Cloud and Microsoft Azure, utilizing container technology for scalability. AI and ML prove effective in classifying threats and improving security, with cloud-based GPUs/TPUs managing resource demands efficiently. The study highlights the robustness and efficiency of AI-driven solutions for cyber security in cloud environments.

In the same year, Filippo Genuario *et. al*, [10] in their study evaluates machine learning-based Intrusion Detection Systems (IDS) for network anomaly detection, comparing machine learning models (e.g., Decision Trees(DT) Random Forest(RF), Naïve Bayes, SVM) and deep learning models (e.g., DNN, CNN, LSTM). They used datasets like KDD-99, NSL-KDD, UNSW-NB15, and IoT-23. The researchers approved the superiority of deep learning models outperform machine learning models, with DNN achieving the highest mean accuracy (95.1%), followed by CNN-LSTM (94.1%). When results indicate SVM has the lowest accuracy (76.0%) and is highly dataset-dependent. The study organized a benchmark, demonstrating the effectiveness of deep learning in intrusion detection and advancing IDS strategies.

While Samer El Hajj Hassan and Nghia Duong-Trung [11] in 2024 applied machine learning techniques to analyze network traffic to enhance cybersecurity and operational efficiency. The proposed work used supervised and unsupervised algorithms, such as logistic regression, random forest, and K-mean, to find anomalies and classify network activities. Their major contributions include developing a dataset standard for identifying malicious network activities, providing. Improving threat detection through improved discrimination between benign and malicious traffic, they also improves anomaly and threat detection capabilities. Providing better insights into network traffic through detailed analysis of patterns and trends in network behavior, which helps prevent and mitigate problems such as congestion and distributed denial of service attacks.

ISSN (online): 2581-3048
Volume 8, Issue 12, pp 11-19, December-2024
https://doi.org/10.47001/IRJIET/2024.812002

Nirvikar Katiyar *et al* [12]. Discussed transformative potential of AI and ML in enhancing cybersecurity by addressing limitations of traditional approaches. They reviewed key ML techniques, real-world applications, challenges, and future research directions. They provid key contributions through an overview of AI/ML applications in cybersecurity, including malware detection, network intrusion detection, fraud detection, and user behavior analytics. The paper demonstrates its ability to identify new and adaptive threats. Thus, organizations can develop proactive, adaptive, and intelligent defenses against evolving cyber threats. However, realizing its full potential requires continued innovation, collaboration, and investment across academia, industry, and government to create a secure digital future.

Anil Kumar Jakkani, [13]. Suggest the algorithms of machine learning (ML) with real-time network traffic analysis and anomaly detection. the model based on some steps of algorithm which feature selection, reduction the dimensions dataset, and compute edge of paradigms to manage large-scale network traffic efficiently. He used UNSW-NB15 datasets, emphasizing automation to enhance real-time intrusion detection and network proactivity, addressing bottlenecks to optimize resource allocation and performance, compute edge for decentralized and faster anomaly detection, achieved the adaption to evolving cyber threats and dynamic network environments.

Prakriti [14] introduce Machine learning (ML) algorithms has emerged as a critical tool for detected cyber threat detection and response against frequency and complexity of cyber threats, such as malware, phishing, ransomware, and advanced persistent threats (APTs). The paper detects rise in cyber threats and hackers' method. The researcher focused to application of cutting-edge, like Random Forest, support vector machine, and deep learning models like CNNs and RNNs, it asserts effectiveness of these algorithms in combating sophisticated cybercriminal activities and the need for ongoing innovation in cybersecurity.

In 2024 Umukoro *et, al.* [15]. Discusses development of an efficient intrusion detection system (IDS) for identifying normal and unusual network traffic patterns. It highlights the use of supervised and unsupervised techniques, leveraging the NSL-KDD dataset and machine learning approaches. The proposed system employs a Genetic Optimization Algorithm (GOA) and Naïve Bayesian (NB) techniques for training and evaluation. Machine learning introduces potential vulnerabilities, such as attackers injecting noisy data into training sets. The paper used GOA to optimize detection accuracy through iterative processes involving crossover and mutation to generate new generations of solutions. Experimental results demonstrate that the GOA-based approach significantly outperforms the Naïve Bayesian method, achieving a detection accuracy of 95% compared to 53.

In 2023 Ajala and Balogun [16] proposed the their paper the role of Machine Learning (ML) in enhancing cybersecurity among growing frequency and complexity of cyber threats. It highlights how advancements in information and communication technologies, especially Internet, have brought substantial benefits but also exposed vulnerabilities, leading to significant financial impacts from cybercrime. The research focuses on practical applications of ML for anomaly detection, threat prediction, and automated response. By analyzing previous studies and real-world cases, it identifies current trends, challenges, and future opportunities for leveraging ML to strengthen cybersecurity strategies in an evolving threat landscape.

In 2021 Sarah *et, al* [17]. Introduce analysis and monitoring for analyzing dynamic, fast-changing network traffic data streams using continuous and adaptive learning strategies. It highlights two challenges: adapting to non-stationary data that evolves over time and addressing the scarcity of labeled data for supervised learning. The authors propose two techniques, ADAM and RAL, to tackle these issues. ADAM uses adaptive memory strategies to adjust to changes in data distribution, while RAL combines reinforcement learning with active learning to reduce the need for labeled data by prioritizing the most informative samples. These methods are applied to real-time detection of network attacks, demonstrating high accuracy despite concept drifts and limited labeled data.

In 2020 Oreja [18]. With other researchers highlights the advancements in deep learning to predication road traffic. They focused both normal and congested traffic conditions. They proposed some technical from deep neural networks for evaluation the highlights depended to common datasets. This paper takes behavior of overall comparison of state-of-the-art models, including new deep neural networks and error recurrent models, using consistent real traffic datasets. They conclude that can used both spatial and temporal traffic dynamics improves prediction accuracy, especially under congestion. The paper cleared eRCNN, outperform standard deep neural networks.

All above works marshaling gathered the overviews of the research works in Network Traffic Analysis arranged in table (1).

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 12, pp 11-19, December-2024

https://doi.org/10.47001/IRJIET/2024.812002

Table 1: Overviews of the research work in Network Traffic Analysis

Reference	Insights	Methods used	Objective	Contribution	Result, future works
Farzaan [9]	AI and ML Enhance Traffic Monitoring • Automates threat detection and response. • Random Forest model achieves 90% accuracy. • Provides solution for cyber threat identification and mitigation.	• AI and ML utilized for cyber incident response system • Random Forest model for Network Traffic Classification and Malware Analysis	• Develop AI-powered cyber incident response system for cloud environments. • Evaluate effectiveness of Random Forest model and Deep Learning models.	• AI-powered system enhances cyber incident response in cloud environments. • Random Forest model achieves high accuracy in threat classification.	• Network Traffic Classifier: 90% accuracy with Random Forest model. • Malware Analysis: 96% accuracy with Dual Model application.
Filippo Genuario [10]	Machine Learning Enhances Traffic Monitoring •Utilizes Decision Trees, Random Forest, and deep learning models. •Detects network anomalies effectively. • Improves response times to cyber threats.	• Shallow learning algorithms: Decision Trees, Random Forest, Naïve Bayes. • Deep learning algorithms: DNN, CNN, LSTM for NIDS tools.	• Compare machine learning-based NIDS for network anomaly detection. • Evaluate deep learning vs. shallow learning algorithms for NIDS.	• Comparative analysis of machine learning-based NIDS tools. • Benchmark development for different proposed strategies.	• Comparative analysis of shallow vs. deep learning NIDS performance. • Lack of focus on specific vulnerabilities in IoT devices.
Samer El Hajj Hassan [11]	Machine Learning Enhances Traffic Monitoring • Analyzes network data for anomaly detection. • Improves threat identification and response. • Reduces network delays. • Improves cybersecurity management performance.	• Logistic regression, decision trees, ensemble learning • Detailed methodology from data preparation to ML model deployment	• Detect anomalies in network traffic using machine learning. • Categorize network activities to enhance security and performance.	• Enhanced network inefficiency identification. • Improved accurate classification of network traffic.	• Enhanced identification of network inefficiencies and traffic classification. • Reduced network delays and improved user satisfaction.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 12, pp 11-19, December-2024

https://doi.org/10.47001/IRJIET/2024.812002

Reference	Insights	Methods used	Objective	Contribution	Result, future works
Nirvikar Katiya [12]	" "AI and ML in Cyber Security" •Focuses on anomaly and network intrusion detection. •Applies to traffic monitoring systems. •Enhances detection and response to cyber threats.. •Doesn't address leveraging machine learning or AI for cyber threats.	• ML algorithms for anomaly detection, malware classification, network intrusion. • Case studies on successful AI/ML implementation in cyber security systems.	• Enhancing threat detection and response with AI/ML. • Exploring AI/ML techniques for cyber security advancements.	• Enhancing threat detection and response with AI and ML. • Overview of current state, techniques, applications, challenges, and future directions.	• AI/ML enhance threat detection and response in cyber security. • Successful implementation in real-world cyber security systems shown.
Anil Kumar Jakkani [13]	Machine Learning and AI in Traffic Monitoring • Automates anomaly detection. • Learns normal traffic patterns. • Enables real-time analysis. • Reduces security risks. • Improves network performance.	• Supervised machine learning techniques for traffic classification. • Algorithms include SVM, Random forests, and neural networks.	• Enhance network security frameworks • Generate insights for better threat prevention mechanisms	• Enhances real-time anomaly detection in complex networks. • Utilizes machine learning for improved network security frameworks.	• Interpretability of machine learning models in network security. • Privacy-preserving methodologies for sensitive network data.
Prakriti Prakriti [14]	"Cyber Threat Detection Using Machine Learning Techniques" •Convolutional Neural Networks and Support Vector Machines effective. •Threat identification and mitigation. • Traffic monitoring systems enhanced.	• ML techniques: CNNs, RNN, Random Forest, SVM • Detect and fight cyber threats effectively.	• Investigate increase in cyber threats and cybersecurity techniques. • Analyze bleeding-edge ML techniques for cyber threat detection.	• ML empowers cyber threat detection and response. • Investigates bleeding-edge ML techniques to fight cyber threats.	• Limited effectiveness of traditional security measures against evolving cyber threats. • Need for continuous innovation to combat sophisticated cybercriminal activities.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 12, pp 11-19, December-2024

https://doi.org/10.47001/IRJIET/2024.812002

Reference	Insights	Methods used	Objective	Contribution	Result, future works
Umukoro [15]	"Network Traffic Analysis Techniques Evolution" • Focuses on intrusion detection system. • Uses Genetic Optimization Algorithm and Naive Bayesian technique. • Aims for efficient network traffic pattern recognition.	• Genetic Optimization Algorithm (GOA) and Naive Bayesian technique • Supervised and unsupervised techniques for network traffic learning patterns	• Create efficient intrusion detection for network traffic patterns. Utilize supervised and unsupervised techniques for detection.	• Developed an efficient intrusion detection system for network traffic patterns. • Achieved 95.0% detection accuracy using Genetic Optimization Algorithm.	• Investigating new attack surfaces introduced by machine learning algorithms. Addressing the influence of noisy data on testing patterns.
Olakunle Abayomi Ajala [16]	"AI and ML in Cybersecurity: Anomaly Detection and Threat Prediction" •Enhances traffic monitoring systems. •Identifies unusual patterns. •Automates responses to cyber threats. • Improves overall security effectiveness.	• AI/ML for anomaly detection, threat prediction, automated response. • Analyzing advancements, outcomes, practical techniques in cybersecurity.	• Explore AI/ML in cybersecurity for anomaly detection and threat prediction. • Analyze real-world implementations and current trends in cybersecurity tactics.	• Role of AI/ML in cybersecurity enhancement. • Techniques for anomaly detection and threat prediction.	• AI/ML enhance anomaly detection, threat prediction, automated response in cybersecurity. • Study uncovers trends, challenges, prospects in cybersecurity tactics with AI/ML.
Sarah Wassermann [17]	Evolution of Network Traffic Analysis Techniques • Shift from offline batch processing to online stream-based approaches. • Enables real-time monitoring and adaptation to concept drifts.	• ADAM: Adaptive memory strategies for dynamically tuning stream-based learning models. • RAL: Reinforcement learning combined with stream-based active learning to reduce labeled data needed.	• Investigate stream-based approaches for network security analysis. • Develop adaptive learning strategies for evolving data challenges.	• Introduces ADAM and RAL for network security analysis. • Evaluates performance on real network attack detection.	• Limited application of stream-based approaches in network security. • Need for improved querying effectiveness in reinforcement learning.

ISSN (online): 2581-3048
Volume 8, Issue 12, pp 11-19, December-2024
https://doi.org/10.47001/IRJIET/2024.812002

Reference	Insights	Methods used	Objective	Contribution	Result, future works
Jesus Mena-Oreja [18]	"Traffic Prediction Techniques Before Deep Learning" • Review of parametric models like autoregressive and Kalman filters. • Highlights limitations. • Emphasizes deep learning's superiority in accurately predicting road traffic dynamics.	• Multilayer perceptron (MLP) for traffic prediction. • Error recurrent models, including eRCNN and LSTM.	• Compare deep neural networks for traffic prediction accuracy. • Evaluate models under normal and congested traffic conditions.	• Comprehensive comparison of deep neural networks for traffic prediction. • Evaluation under normal and congested traffic conditions.	• Lack of evaluation under common datasets for congestion prediction. • Insufficient focus on congestion formation prediction techniques.

IV. CONCLUSION

In last decade form 20th, the networks were developed greatly and extensively at all levels. It interested many researchers in analysis and prediction of network traffic in their subjects, and it became continuous research in various sub-fields. They implement a lot of papers for effective network traffic algorithms, analysis, balanced loading of network, and prediction of network traffic. This paper surveyed several of the more important network traffic with artificial intelligence algorithms, such as machine learning, ensemble learning, and deep learning. The tabular marshaling gave an overview of the research work in this field; it contains the summarized points such as dataset, algorithms, performance metrics, and results. This paper issues intuition about topic to new researchers.

ACKNOWLEDGEMENT

I would like to express my deepest thanks, appreciation, and gratitude to my dear professor, Ibrahim Ahmed Saleh, for his continuous support in my research career and for his valuable comments on both the life and scientific levels.

REFERENCES

[1] M. Abbasi, A. Shahraki, and A. Taherkordi, "Deep Learning for Network Traffic Monitoring and Analysis (NTMA): A Survey," *Comput. Commun.*, vol. 170, no. September 2020, pp. 19–41, Mar. 2021, doi: 10.1016/j.comcom.2021.01.021.

[2] Y. Yang, "Application of Data Mining Algorithm in Network Security Detections," *Highlights Sci. Eng. Technol.*, vol. 85, pp. 920–923, 2024, doi: 10.54097/19hgwb09.

[3] H. Huang, S. Chen, R. Ben Basat, H. Dai, A. Taherkordi, and J. Xu, "Guest Editorial Introduction to the Special Section on Next-Generation Traffic Measurement With Network-Wide Perspective and Artificial Intelligence," *IEEE Trans. Netw. Sci. Eng.*, vol. 11, no. 3, pp. 2332–2337, 2024, doi: 10.1109/TNSE.2024.3389428.

[4] N. Anderson, M. Li, and M. Evans, "Mapping the Ransomware Ecosystem: Tracing Network Traffic to Command & Control Centers." Sep. 10, 2024. doi: 10.36227/techrxiv.172599578.85351154/v1.

[5] S. Zavrak and M. Iskefiyeli, "Anomaly-Based Intrusion Detection from Network Flow Features Using Variational Autoencoder," *IEEE Access*, vol. 8, pp. 108346–108358, 2020, doi: 10.1109/ACCESS.2020.3001350.

[6] B. Wu, J. Xu, Y. Zhang, B. Liu, Y. Gong, and J. Huang, "Integration of computer networks and artificial neural networks for an AI-based network operator," *Appl. Comput. Eng.*, vol. 64, no. 1, pp. 115–120, 2024, doi: 10.54254/2755-2721/64/20241370.

[7] S. Geißler *et al.*, "Untangling IoT Global Connectivity: The Importance of Mobile Signaling Traffic," *IEEE Trans. Netw. Serv. Manag.*, vol. 21, no. 4, pp. 4435–4449, Aug. 2024, doi: 10.1109/TNSM.2024.3414975.

[8] S. Ullah Khan, Z. Ulalh Khan, M. Alkhowaiter, J. Khan, and S. Ullah, "Energy-efficient routing protocols for UWSNs: A comprehensive review of taxonomy, challenges, opportunities, future research directions, and machine learning perspectives," *J.*

ISSN (online): 2581-3048
Volume 8, Issue 12, pp 11-19, December-2024
https://doi.org/10.47001/IRJIET/2024.812002

King Saud Univ. - Comput. Inf. Sci., vol. 36, no. 7, 2024, doi: 10.1016/j.jksuci.2024.102128.

[9] M. A. M. Farzaan, M. C. Ghanem, A. El-Hajjar, and D. N. Ratnayake, "AI-Enabled System for Efficient and Effective Cyber Incident Detection and Response in Cloud Environments," pp. 1–18, 2024, [Online]. Available: http://arxiv.org/abs/2404.05602

[10] F. Genuario, G. Santoro, M. Giliberti, S. Bello, E. Zazzera, and D. Impedovo, "Machine learning-based methodologies for cyber-attacks and network traffic monitoring." IEEE, Jul. 01, 2024. doi: 10.20944/preprints202407.0029.v1.

[11] S. E. H. Hassan and N. Duong-Trung, "Machine Learning in Cybersecurity: Advanced Detection and Classification Techniques for Network Traffic Environments," *EAI Endorsed Trans. Ind. Networks Intell. Syst.*, vol. 11, no. 3, pp. 1–22, 2024, doi: 10.4108/eetinis.v11i3.5237.

[12] D. N. Katiyar, M. S. Tripathi, M. P. Kumar, M. S. Verma, D. A. K. Sahu, and D. S. Saxena, "AI and Cyber-Security: Enhancing threat detection and response with machine learning.," *Educ. Adm. Theory Pract.*, vol. 30, no. 4, pp. 6273–6282, 2024, doi: 10.53555/kuey.v30i4.2377.

[13] A. K. Jakkani, "Real-Time Network Traffic Analysis and Anomaly Detection to Enhance Network Security and Performance: Machine Learning Approaches," *J. Electron. Netw. Appl. Math.*, no. 44, pp. 32–44, 2024, doi: 10.55529/jecnam.44.32.44.

[14] P. Prakriti, "Cyber Threat Detection Using Machine Learning," *Interantional J. Sci. Res. Eng. Manag.*, vol. 08, no. 07, pp. 1–15, 2024, doi: 10.55041/ijsrem36799.

[15] I. I. Umukoro, B. O. Eke, and O. Edward, "An efficient intrusion detection technique for traffic pattern learning," *Sci. Africana*, vol. 23, no. 2, pp. 25–40, 2024, doi: 10.4314/sa.v23i2.3.

[16] Olakunle Abayomi Ajala and Olusegun Abiodun Balogun, "Leveraging AI/ML for anomaly detection, threat prediction, and automated response," *World J. Adv. Res. Rev.*, vol. 21, no. 1, pp. 2584–2598, 2024, doi: 10.30574/wjarr.2024.21.1.0287.

[17] S. Wassermann, T. Cuvelier, P. Mulinka, and P. Casas, "Adaptive and Reinforcement Learning Approaches for Online Network Monitoring and Analysis," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 2, pp. 1832–1849, 2021, doi: 10.1109/TNSM.2020.3037486.

[18] J. Mena-Oreja and J. Gozalvez, "A Comprehensive Evaluation of Deep Learning-Based Techniques for Traffic Prediction," *IEEE Access*, vol. 8, pp. 91188–91212, 2020, doi: 10.1109/ACCESS.2020.2994415.

AUTHORS BIOGRAPHY

Osama Yassin Mohammed, Assistant Lecturer in the Department of Computer Systems Technologies at Northern Technical University, Mosul, Iraq, a position he has held since June 2011. He earned an MSc in Computer Science from the University of Mosul in October 2010 and is currently pursuing a Ph.D. in Computer Science at the same university, starting in September 2021. His research focuses on addressing modern challenges in computer science and artificial intelligence. E-mail: osama.21csp75@student.uomosul.edu.iq

Ibrahim Ahmed Saleh, was born in Mosul-Iraq in 1963. He received his MSc. degree (in signal and image processing) from the University of Mosul, Iraq in 2003 and in 2013 he received his PhD inartificial techniques and computer networking from Mosul University. He became professor in 2021. From 1997 to 2005, he worked at computer center in Mosul University/Iraq. Currently he is professor at the Dept. of Software Engineering, College of Computer Sciences and Math, and University of Mosul, Iraq. He can be contacted at email: i.hadedi@uomosul.edu.iq

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 12, pp 11-19, December-2024

https://doi.org/10.47001/IRJIET/2024.812002

Citation of this Article:

Osama Yassin Mohammed, & Ibrahim Ahmed Saleh. (2024). Survey of Computer Network Traffic Analysis Using Artificial Intelligence Algorithms. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 8(12), 11-19. Article DOI https://doi.org/10.47001/IRJIET/2024.812002

****

