AI-Powered Network Traffic Management for Modern Digital Infrastructures: A Comprehensive Survey

K. Praveen Kumar, H. Murahari Krishna
Department of Electronics & Telecommunication BVCOEW, SPPU Pune – India

Abstract:

The rapid digital transformation driven by emerging technologies such as IoT, 5G, and edge computing has drastically increased network traffic complexity. Traditional traffic management techniques struggle to cope with evolving patterns, diverse QoS demands, and growing cyber threats. This paper surveys the role of Artificial Intelligence (AI) and Machine Learning (ML) in network traffic optimization, anomaly detection, and intrusion prevention across modern digital infrastructures. We analyze AI-powered methods like deep learning, federated learning, and hybrid neural architectures, discuss key challenges such as data privacy, and propose future directions for adaptive, intelligent network management systems.

Keywords: Network Traffic Optimization, Artificial Intelligence, Machine Learning, IoT Networks, Edge Computing, Intrusion Detection, Federated Learning, Deep Learning, Cybersecurity.

1. Introduction

The digital revolution has deeply transformed industries, leading to massive data generation and exchange across enterprise, cloud, and telecommunication networks [1]. The proliferation of IoT, 5G, and edge computing technologies has intensified network traffic, making traditional management methods insufficient.

Static, rule-based network management strategies are no longer effective due to the unpredictable nature of modern network traffic and increasing cybersecurity threats [2]. In order to ensure dependable and effective digital communications, AI and ML approaches are being used to automate and optimize network traffic management procedures in real-time. [3].

This research paper aims to provide a comprehensive overview of AI-powered solutions for network traffic optimization, review recent advances, and highlight ongoing challenges and future research directions.

2. Literature Review

2.1 5G Network Optimization

The increasing complexity of managing 5G networks, driven by their full-scale deployment and the unprecedented speed, capacity, and ultra-low latency they offer, is being addressed through the application of artificial intelligence (AI) and machine learning (ML) [4]. 5G network design and maintenance are being revolutionized by AI-

driven solutions that make predictive, adaptive, and extremely effective management possible [5]. Key AI and ML techniques employed in 5G network optimization, along with their respective advantages, are detailed below:

Predictive Analytics for Network Demand Forecasting: Predictive analytics is crucial for anticipating network demand, allowing operators to proactively adjust resources and mitigate congestion [6]. These models analyze usage trends, seasonal variations, and contextual factors to provide accurate predictions, empowering network operators to ensure consistent performance across varying conditions and minimizing outages or overloads, particularly during peak demand.

Reinforcement Learning for Adaptive Network Management: Reinforcement learning (RL), a subfield of machine learning, is employed for adaptive network management [8]. This process enables the agent to learn optimal strategies for network condition optimization. In 5G, RL facilitates dynamic spectrum allocation and adaptive power control.

Traffic Analysis and Management:

Neural networks, particularly deep learning models, are used to enhance traffic analysis and management [9]. Deep learning models, with their hierarchical processing of data through multiple layers of neurons, can analyze complex data patterns and extract meaningful insights for network optimization [10]. Classifying traffic and detecting anomalies is a crucial use of deep learning in 5G [11]. By processing large volumes of data from network nodes, these models identify patterns associated with normal traffic flow and detect anomalies indicative of issues such as cyberattacks or network congestion. Additionally, deep learning models make it possible for application-based traffic shaping, which prioritizes bandwidth and resource allocation for the best user experience by managing various traffic types (such as voice calls, video streaming, and IoT data) depending on their unique needs [12].

Examples:

Support Vector Machines (SVMs) are employed for classification tasks, such as identifying specific or malicious traffic types [13]. K-Means clustering is used to segment network traffic based on similarities, enabling personalized network services and optimized resource allocation [14]. Random forests, which are decision-tree-based models, predict network traffic, classify network activities, and detect anomalies for faster issue identification and mitigation [15]. Recurrent Neural Networks (RNNs) are valuable for time-series forecasting, facilitating the prediction of network traffic based on historical patterns and enabling operators to anticipate peak demand periods for proactive resource allocation [16]. The integration of these models into network management systems enhances the efficiency, security, and resilience of 5G networks [17].

Advantages of Using AI for Resource Allocation and Load Balancing: AI-driven solutions offer several advantages for resource allocation and load balancing in 5G networks, including:

Real-Time Decision Making: AI algorithms process data in real-time, enabling instantaneous network adaptation to changing conditions, which is crucial for applications with stringent latency requirements, such as autonomous vehicles and remote surgery.

Enhanced Scalability: AI-driven models efficiently manage increased loads as networks grow in size and complexity, ensuring optimal resource allocation. For 5G networks to support the vast number of connected devices, this scalability is crucial.

Reduced Operational Costs: The automation of tasks like spectrum management and

power control through AI reduces the need for manual intervention, lowering operational costs. AI-powered predictive maintenance also minimizes downtime and associated costs by identifying potential issues proactively.

Improved User Experience: AI-driven resource allocation and load balancing ensure consistent, high-quality service delivery, even during peak times, by distributing traffic evenly across network resources and preventing bottlenecks.

Energy Efficiency: AI optimizes energy consumption in 5G networks by dynamically adjusting power levels based on network demand, leading to both cost reduction and a minimized environmental impact.

2.2 Machine Learning in Traffic Analysis

ML algorithms are widely used for detecting anomalies and optimizing traffic flows. Techniques like clustering, classification, and regression models enable dynamic traffic prediction and congestion management [18].

Application

Machine learning (ML) is increasingly employed in network traffic analysis to automate operational processes, enhance accuracy, and bolster network security. ML algorithms facilitate the classification of network traffic, detection of anomalies, and prediction of future traffic patterns, thereby improving overall network performance and security.

The following details the specific applications of machine learning in this domain:

Network Traffic Classification: ML algorithms, such as Support Vector Machines (SVMs) and Decision Trees, are trained to categorize network traffic. This categorization is based on a variety of features, including protocol, source and destination IP addresses, and port numbers. This enables a more effective understanding of network traffic patterns, which can be utilized to identify malicious activity and optimize resource allocation.

Anomaly Detection: Unsupervised learning techniques, including clustering and other anomaly detection methodologies, are used to identify unusual or unexpected traffic patterns. These trends could point to possible security risks or deterioration in performance. The detection of these anomalies by ML models contributes to the prevention of data breaches and the enhancement of network security.

Traffic Prediction: ML algorithms, including regression and time series models, are applied to predict future traffic patterns. These predictions are based on historical data and enable network administrators to proactively prepare for periods of high traffic volume, optimize resource allocation, and prevent network congestion.

Security Applications: ML is utilized in the detection of various network security threats, including intrusion detection, malware analysis, and botnet detection. By analyzing network traffic patterns, ML models can identify malicious activities and thereby help to prevent data breaches.

Tools and Techniques: Commonly employed ML algorithms in this context include Support Vector Machines (SVMs), Decision Trees, Random Forests, and various deep learning models. These ML models are trained and evaluated using network traffic data that has been captured and analyzed using tools like Wireshark. Additionally, AI-powered tools are available for continuous network traffic monitoring and analysis.

Benefits: The application of ML in network traffic analysis provides several key benefits: Increased accuracy in the detection of anomalies and security threats. Enhanced scalability to effectively manage high

volumes of network traffic. Improvement in overall network performance and efficiency.

2.3 Deep Learning Architectures

Deep Learning (DL) models, particularly Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), enhance traffic pattern recognition and intrusion detection. When applied to sequential and high-dimensional network data, DL models perform exceptionally well. [19].

2.4 Federated Learning for Privacy Preservation

Federated learning (FL) addresses data privacy concerns by training models locally and aggregating updates centrally without sharing raw data [20]. This approach is particularly beneficial for IoT ecosystems where data privacy is critical.

3. Methodologies and Case Studies

3.1 P2P Detection using Logistic Regression and SOM-MLP Hybrid

Sowah et al. [21] proposed logistic regression and a hybrid Self Organizing Map (SOM)–Multi-Layer Perceptron (MLP) model for P2P traffic detection. Detection accuracies were impressive, reaching 99.93% in some instances, highlighting the potential of hybrid unsupervised-supervised techniques.

3.2 Multilevel Cyberattack Detection using RNN-LSTM-GRU

Ayodele and Buttigieg [22] developed stacked RNN, LSTM, and GRU models for multi-level cyberattack detection at packet, flow, and session layers, achieving up to 99.99% classification accuracy.

3.3 Traffic Sign Recognition Enhancement with ANN

Amos et al. [23] improved traffic sign recognition using a Novel Artificial Neural Network (ANN) achieving 90.58% accuracy, significantly outperforming RNNs.

3.4 CNN-LSTM for Traffic Anomaly Detection

Brych et al. [24] applied CNN and LSTM models for traffic classification. LSTM models exhibited better generalization on sequential data compared to CNNs, achieving validation accuracy up to 64%.

3.5 Federated Learning and ELM for Traffic Classification

Qiu [25] proposed the NTFLELM model, achieving a 12% accuracy improvement over traditional methods, showcasing the effectiveness of privacy-preserving distributed learning.

3.6 URL Malicious Detection using Network Traffic Features

Fadheel et al. [26] compared different feature selection techniques (Complete, KMO, PCA) and classifiers (SVM, KNN, LR) for detecting malicious URLs. Results favored network traffic features, achieving up to 95% accuracy.

3.7 Periodic Behavioral Pattern Detection with XGBoost

Koumar and Cejka [27] exploited time series autocorrelation and trained XGBoost classifiers to detect periodic communication patterns, achieving a 90% F1-score.

4. Edge Computing, Fog Computing, and IoT Traffic Management

IoT devices, with limited computation capacities, heavily rely on network connectivity for data exchange. Cloud load and latency can be reduced with the use of edge and fog computing models. [28].

Capturing traffic at different layers—application, transport, and network—enables richer feature extraction for device identification and security analysis [29].

Edge and Fog Computing in IoT Traffic Management

These paradigms facilitate data processing closer to the source, thereby reducing latency and enhancing real-time decision-making capabilities within domains such as smart cities.

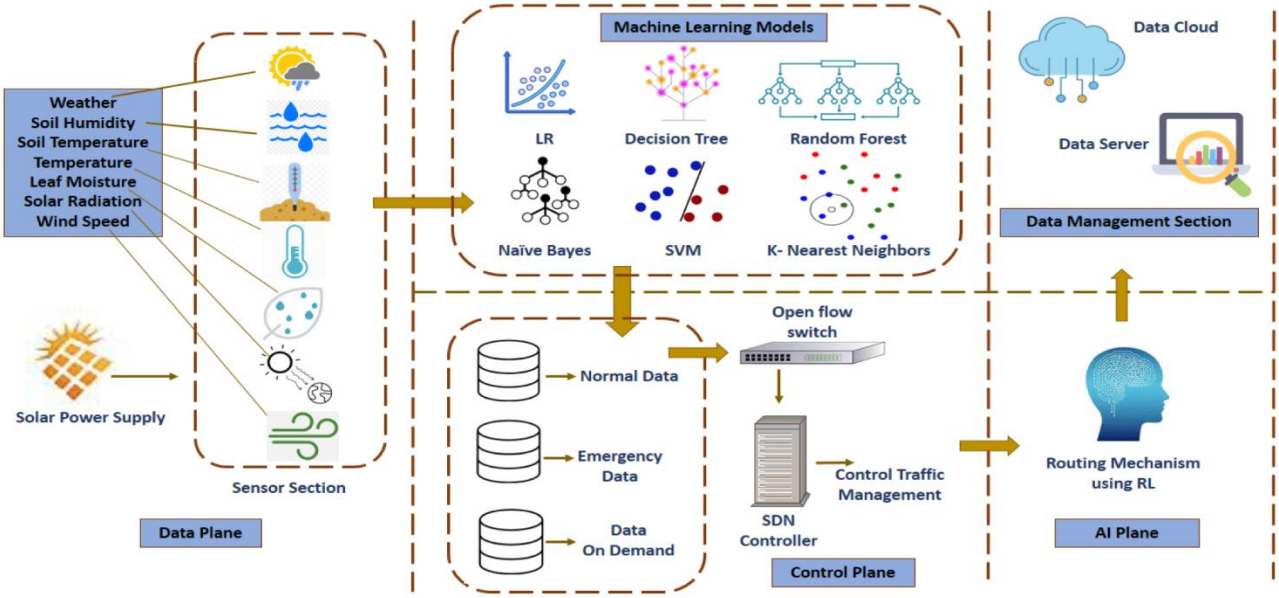

Image source: https://www.mdpi.com/1424-8220/23/19/8218

Edge Computing:

Benefits: Lower latency, faster response times, improved security and privacy through local data processing, and reduced bandwidth consumption.

Fog Computing:

Focus: A distributed computing architecture that creates a processing layer between edge devices and the cloud, extending cloud capabilities to the network edge.

Benefits: Enables more complex data processing at the edge, facilitates resource sharing among devices, and enhances the scalability and reliability of IoT systems.

Applications: Smart city management, industrial automation, and connected vehicle systems.

IoT Traffic Management:

Focus: Uses Internet of Things sensors and gadgets to collect information about infrastructure, cars, and traffic conditions, allowing for real-time administration and monitoring.

Benefits: Improves traffic flow, reduces congestion, enhances safety, and enables more efficient resource allocation.

Integration with Edge/Fog Computing:

Real-time analysis and decision-making for efficient traffic management are made possible by this combination.

In essence: Edge computing handles data processing at the source, whereas fog computing offers a more centralized processing layer situated between edge devices and the cloud. Both are indispensable for achieving efficient IoT traffic management, facilitating real-time data analysis, improved decision-making, and enhanced traffic flow.

5. Results and Discussion

Technique	Accuracy (%)	Notes
SOM-MLP Hybrid for P2P	99.93	Excellent P2P identification
RNN-LSTM-GRU Stack	99.99	Multilevel cyberattack detection
ANN for Traffic Signs	90.58	Higher than RNN (76.65)
CNN-LSTM for Traffic Classification	64 (LSTM Validation)	Sequential data advantage
Federated ELM (NTFLELM)	+12% over benchmarks	Privacy-preserving
URL Detection (PCA-KNN)	95	Lexical feature best combination
XGBoost for Periodic Patterns	90 (F1-score)	Time series-based

AI-based approaches consistently outperform traditional rule-based methods, offering adaptive learning and real-time decision-making capabilities.

COMPARISON BETWEEN VARIOUS ML MODELS FOR NETWORK TRAFFIC ANALYSIS

Models	Accuracy	Precision	Recall	F1-score
GRU [18]	77	67	75	65
LR[19]	92.8	92.83	92.8	92.8
LSTM[20]	94.73	91.09	92.55	93.3
CNN	**99**	**99.03**	**98.86**	**99**

Table source: https://www.ijsat.org/papers/2025/2/3428.pdf

6. Challenges in AI-based Network Traffic Management

AI-based network traffic management faces several key challenges: data privacy and security concerns, high implementation costs, integration with legacy systems, the potential for algorithm bias, and the need for robust maintenance and reliability. Additionally, public acceptance, ethical considerations, and the complexity of managing diverse networks contribute to the overall complexity.

Detailed Challenges:
Data Privacy and Security: AI systems rely on vast amounts of data, including real-time traffic information and potentially personal data, raising significant privacy and security concerns. It is essential to make sure that this sensitive data is shielded against abuse and illegal access.

Implementation Costs: Deploying AI-based traffic management systems, including sensors, cameras, and communication networks, can be expensive. Developing nations may face challenges in allocating sufficient funding.

Integration with Legacy Systems: AI solutions may not be compatible with current traffic management systems, necessitating significant changes and sometimes intricate implementations.

Algorithm Bias: AI models trained on biased datasets may produce skewed results, potentially favoring certain routes or neglecting underrepresented areas.

Public Acceptance: For AI systems to be effective, public trust and confidence are essential. Residents must feel that these technologies improve their lives without compromising privacy or safety.

Ethical Considerations: AI systems can be scrutinized due to trust and explainability issues. Algorithm bias can lead to discriminatory outcomes, requiring careful design and development.

Infrastructure Challenges: The incorporation of AI-driven solutions may be hampered by antiquated and incompatible traffic management systems.

Data Quality and Complexity: AI models rely on high-quality data, and the complexity and diversity of data sources can be challenging to manage.

Network Complexity and Variability: Managing the complexity and diversity of networks while dealing with uncertainty and variability requires careful attention.

Scalability: AI systems need to be able to handle increased loads as cities and networks grow.

7. Future Directions

- **Hybrid Deep Learning Models:** These models integrate Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTMs) networks to improve feature extraction and sequential data learning. This combination enables more effective analysis of complex traffic patterns.
- **Lightweight Edge AI Models:** Research is focused on developing resource-efficient AI models optimized for real-time inference at the network edge. This is crucial for applications with low-latency requirements and limited computational resources.
- **Self-Supervised Learning:** Methodologies are being developed to reduce the reliance on labeled datasets. Self-supervised learning techniques

allow models to learn from unlabeled data, addressing the challenge of data scarcity in many network environments.

- **Explainable AI (XAI):** Efforts are being made to enhance model interpretability. By offering insights into how models arrive at their findings, XAI seeks to increase security and encourage better confidence by making AI judgments more transparent and intelligible.
- **Federated Adversarial Training:** Techniques are being developed to improve the robustness of federated learning systems against cyberattacks. Federated adversarial training aims to make distributed AI systems more resilient to malicious manipulation.
- **6G Networks and AI Synergy:** Research is underway to prepare for the integration of AI layers into future ultra-dense, ultra-low latency 6G network environments. This integration seeks to optimize the performance and management of these advanced networks.

8. Conclusion

The integration of AI into network traffic management marks a pivotal shift in ensuring efficient, secure, and scalable digital infrastructures. Emerging AI techniques such as deep learning, federated learning, and hybrid architectures have demonstrated significant potential in enhancing network performance, anomaly detection, and security enforcement. Nonetheless, issues with generalization, computational complexity, and data privacy continue to exist. Future research should focus on lightweight, explainable, and privacy-preserving AI models to fully realize the vision of autonomous, intelligent network management systems for the next generation of digital transformation.

Published research has extensively addressed the problems of device identification based on traffic classification and intruder detection based on traffic prediction, utilizing traffic traces of Internet of Things (IoT) devices. However, more thorough research is required on subjects like federated learning applications in 5G and 6G networks, traffic tracing, traffic classification, and traffic prediction. Modern networks face significant challenges, including unreliability and safety issues, with various attack activities posing threats. Network performance analysis is further complicated by the fundamental issues of performance, privacy, latency, and control overhead requirements in real-world networks. For the purpose of identifying irregularities, keeping an eye on network availability, and optimizing network performance, traffic pattern analysis is essential.

References

[1] Küng, Lucy, Anna-Martina Kröll, Bettina Ripken, and Marcel Walker. "Impact of the digital revolution on the media and communications industries." Javnost-the Public 6, no. 3 (1999): 29-47.
[2] George, A. Shaji, T. Baskar, P. Balaji Srikaanth, and Digvijay Pandey. "Innovative Traffic Management for Enhanced Cybersecurity in Modern Network Environments." Partners Universal International Research Journal 3, no. 4 (2024): 1-13.
[3] Karamchand, Gopal Krishna. "Networking 4.0: The Role of AI and Automation in Next-Gen Connectivity." Journal of Big Data and Smart Systems 5, no. 1 (2024).
[4] Esenogho, Ebenezer, Karim Djouani, and Anish M. Kurien. "Integrating artificial intelligence Internet of Things and 5G for next-generation smartgrid: A survey of

trends challenges and prospect." Ieee Access 10 (2022): 4794-4831.
[5] PireciSejdiu, Nora, Nikola Rendevski, and Blagoj Ristevski. "AI Revolutionizing 5G and Next-Generation Networks." In 2024 IEEE 17th International Scientific Conference on Informatics (Informatics), pp. 331-336. IEEE, 2024.
[6] Abdullah, Ahmad Faizal. "Big Data Analytics for Enhanced Traffic Flow Optimization in Urban Transportation Networks." Journal of Applied Cybersecurity Analytics, Intelligence, and Decision-Making Systems 14, no. 12 (2024): 45-53.
[7] Ma, Bo, Weisi Guo, and Jie Zhang. "A survey of online data-driven proactive 5G network optimisation using machine learning." IEEE access 8 (2020): 35606-35637.
[8] Shahraki, Amin, Torsten Ohlenforst, and Felix Kreyß. "When machine learning meets network management and orchestration in edge-based networking paradigms." Journal of Network and Computer Applications 212 (2023): 103558.
[9] Almukhalfi, Hanan, Ayman Noor, and Talal H. Noor. "Traffic management approaches using machine learning and deep learning techniques: A survey." Engineering Applications of Artificial Intelligence 133 (2024): 108147.
[10] Sarker, Iqbal H. "Deep learning: a comprehensive overview on techniques, taxonomy, applications and research directions." SN computer science 2, no. 6 (2021): 1-20.
[11] Doan, Minh, and Zhanyang Zhang. "Deep learning in 5G wireless networks-anomaly detections." In 2020 29th Wireless and Optical Communications Conference (WOCC), pp. 1-6. IEEE, 2020.
[12] Barakabitze, Alcardo Alex, Nabajeet Barman, Arslan Ahmad, Saman Zadtootaghaj, Lingfen Sun, Maria G. Martini, and Luigi Atzori. "QoE management of multimedia streaming services in future networks: A tutorial and survey." IEEE Communications Surveys & Tutorials 22, no. 1 (2019): 526-565.
[13] Boualouache, Abdelwahab, and Thomas Engel. "A survey on machine learning-based misbehavior detection systems for 5g and beyond vehicular networks." IEEE Communications Surveys & Tutorials 25, no. 2 (2023): 1128-1172.
[14] Zhao, Shasha, Yi Xiao, Yueqiang Ning, Yuxiao Zhou, and Dengying Zhang. "An optimized K-means clustering for improving accuracy in traffic classification." Wireless personal communications 120 (2021): 81-93.
[15] Azam, Zahedi, Md Motaharul Islam, and Mohammad Nurul Huda. "Comparative analysis of intrusion detection systems and machine learning-based model analysis through decision tree." IEEE Access 11 (2023): 80348-80391.
[16] He, Yuxin, Ping Huang, Weihang Hong, Qin Luo, Lishuai Li, and Kwok-Leung Tsui. "In-depth insights into the application of recurrent neural networks (rnns) in traffic prediction: A comprehensive review." Algorithms 17, no. 9 (2024): 398.
[17] Khan, Rafiq Ahmad, Habib Ullah Khan, Hathal Salamah Alwageed, Hussain A. Alhashimi, and Ismail Keshta. "5G Networks Security Mitigation Model: An ANN-ISM Hybrid Approach." IEEE Open Journal of the Communications Society (2025).
[18] Laanaoui, My Driss, Mohamed Lachgar, Hanine Mohamed, Hrimech Hamid, Santos Gracia Villar, and Imran Ashraf. "Enhancing Urban Traffic Management Through Real-Time Anomaly Detection and Load Balancing." Ieee Access (2024).
[19] Elsayed, Salwa, Khalil Mohamed, and Mohamed Ashraf Madkour. "A comparative study of using deep learning algorithms in

network intrusion detection." IEEE Access 12 (2024): 58851-58870.
[20] Liu, Ziyao, Jiale Guo, Wenzhuo Yang, Jiani Fan, Kwok-Yan Lam, and Jun Zhao. "Privacy-preserving aggregation in federated learning: A survey." IEEE Transactions on Big Data (2022).
[21] Sowah, Robert A., Godfrey A. Mills, Emmanuel Togo, Pamela Pomary, and Gifty Osei. "Efficient Computer Networks Peer-To-Peer (P2P) Traffic Management and Control Using Machine Learning with Open Source Tools." In 2024 IEEE 9th International Conference on Adaptive Science and Technology (ICAST), vol. 9, pp. 1-6. IEEE, 2024.
[22] Ayodele, Believe, and Victor Buttigieg. "A Multi-Level Network Traffic Classification in Combating Cyberattacks Using Stack Deep Learning Models." In 2024 8th Cyber Security in Networking Conference (CSNet), pp. 143-146. IEEE, 2024.
[23] Amos, P., S. Narendran, and M. Keerthivasan. "Analysis Of Traffic Sign Recognition Using Artificial Neural Network Algorithm Compared With Accuracy Of Recurrent Neural Networks." In 2024 9th International Conference on Applying New Technology in Green Buildings (ATiGB), pp. 502-506. IEEE, 2024.
[24] Brych, Petro, Serhii Pryshlyak, Oleksii Kovalisko, Denys Markiv, Gennadii Boikachov, and Mykola Brych. "A Study of Traffic Analysis Algorithms in Telecommunication Networks Using Deep Learning to Identify and Classify Data Types." In 2024 IEEE 17th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), pp. 1-4. IEEE, 2024.
[25] Qiu, Cheng. "A network traffic classification method based on federated learning and extreme learning machine." In 2023 IEEE International Conference on Control, Electronics and Computer Technology (ICCECT), pp. 284-289. IEEE, 2023.
[26] Fadheel, Wesam, Wassnaa Al-Mawee, and Steve Carr. "On phishing: Url lexical and network traffic features analysis and knowledge extraction using machine learning algorithms (a comparison study)." In 2022 5th International Conference on Data Science and Information Technology (DSIT), pp. 1-7. IEEE, 2022.
[27] Koumar, Josef, and Tomáš Čejka. "Network traffic classification based on periodic behavior detection." In 2022 18th International Conference on Network and Service Management (CNSM), pp. 359-363. IEEE, 2022.
[28] Angel, Nancy A., Dakshanamoorthy Ravindran, PM Durai Raj Vincent, Kathiravan Srinivasan, and Yuh-Chung Hu. "Recent advances in evolving computing paradigms: Cloud, edge, and fog technologies." Sensors 22, no. 1 (2021): 196.
[29] Shen, Meng, Ke Ye, Xingtong Liu, Liehuang Zhu, Jiawen Kang, Shui Yu, Qi Li, and Ke Xu. "Machine learning-powered encrypted network traffic analysis: A comprehensive survey." IEEE Communications Surveys & Tutorials 25, no. 1 (2022): 791-824.