

INTERNATIONAL JOURNAL OF INNOVATIONS IN SCIENCE & TECHNOLOGY AI-DRIVEN NETWORK TRAFFIC MONITORING AND VISUALIZATION SYSTEM USING A HYBRID XGBOOST AND DEEP AUTOENCODER FRAMEWORK

Muhammad Awais Hassan¹, Fawad Nasim^{1,*}, Arshad Mahmood¹

¹Faculty of Computer Science and Information Technology, The Superior University, Lahore, 54600, Pakistan.

*fawad.nasim@superior.edu.pk

DOI: <https://doi.org/10.5281/zenodo.22094066>

Keywords

Network Traffic Monitoring, Artificial Intelligence, XGBoost, Deep Autoencoder, Intrusion Detection, CIC-IDS-2018, WebSockets, D3.js, Network Visualization.

Article History

Received: 28 April 2026

Accepted: 15 June 2026

Published: 30 June 2026

Copyright ©Author

Corresponding Author: *

Fawad Nasim

Abstract

Enterprise, cloud and IoT networks are generating lots of traffic, which are hard to monitor. We believe that the proposed XGBoost-Supervised Anomaly Detection (SA) and Deep Autoencoder-Unsupervised (UAE) based AI network traffic monitoring and visualization system would be beneficial. The system processes live packet streams, NetFlow/IPFIX files or historical PCAP data, aggregates packets into bi-directional flows, fetches 42 statistical and temporal data features, and uses a two-stage AI analytics pipeline. Real-time alerting and fastAPI backend and WebSocket topology views. Test is accomplished using the CIC-IDS-2018 benchmark and simulated live packet streams. The proposed XGBoost classifier gets 99.45% accuracy and 99.45% F1-score on 1.8 ms of the previously unseen anomalous behavior. The reported processing components end-to-end are in millisecond level latency and the dashboard fully supports the quick interpretation of the network events. The outcome indicate that employing supervised classification, unsupervised anomaly scoring and real-time visualization can create a useful monitoring framework for security operations.

1. Introduction

1.1 Background and Motivation

The amount and complexity of network traffic is growing rapidly with the development of digital networks, cloud computing, Internet of Things (IoT) and smart transportation systems[1],[2]. The traditional network monitoring methods are increasingly being put to the test for their ability to process high speed traffic [3], detect abnormal behavior and timely information to the administrator and security analyst [4]. Therefore, the last few years have seen the integration of Artificial Intelligence (AI)[5], Machine Learning (ML)[6], deep learning [7] and enhanced visualization capabilities in network traffic monitoring and management systems[8],[9].

AI driven techniques have been demonstrated to have great potential for the analysis of complex and large-scale traffic data [10]. Sujakumari and Dassan[11] explored the use of Generative Adversarial Networks (GAN) and real-time traffic prediction with HDFS, demonstrating how AI techniques can be used to handle large-scale traffic data and improve the accuracy of real-time traffic predictions . In the same vein, Jaramillo-Alcazar et al. investigated the possibility of implementing blockchain-enabled computer vision and intelligent technologies for smart city traffic optimization highlighting the need for the integration of various technologies to improve intelligent traffic-management systems [12]. Naveed et al. [13] proposed an intelligent

traffic surveillance system using wireless sensor networks with advanced phase-timing optimization, which highlighted the potential of sensor systems for intelligent and adaptive traffic monitoring.

Moreover, there has been a large body of research on the use of machine learning in traffic analysis. Bustamante-Bello et al. presented a study of machine learning techniques for anomaly detection and visualization for street pavements using Fog Computing and vehicle-to-infrastructure (V2I) networks, highlighting the benefits of combining distributed computing, sensing, machine learning and visualization to enable real time monitoring applications [14]. In the field of cybersecurity[15],[16], Salau and Beyene[17] explored how machine learning methods can be applied to classify network traffic in SDN systems, demonstrating that there is a possibility to use a standard ML models[18] to classify network traffic in modern programmable networks. Dhakad et al. surveyed the AI, ML, and DL methods for real-time network traffic analysis highlighting the feasibility of applying them to large and fast networks [19].

The networks are increasingly becoming a challenge for traditional monitoring systems because of the increasing amount and speed of network traffic[20]. Akshatha V and Srinivasan[21] have been working on AI based network traffic analysis for large scale and high speed traffic environments and emphasized on the need of intelligent methods to deal with complex network data. Similarly, Priya gave a talk on the use of machine learning and artificial intelligence in network traffic anomaly detection and the importance of detecting abnormalities in the network traffic to enhance network security and reliability [22]. Research indicates the use of automated anomaly detection[23] can help decrease manual traffic review and enhance the detection of potentially anomalous traffic by network administrators.

Besides detection and classification, visualization is one of the crucial aspects of today's network monitoring. Kapadia et al. [24] studied visualization of data and preprocessing for network traffic analysis in the framework of

cybersecurity. They demonstrated that effective visualization[25] can assist analysts in comprehending the traffic data and identifying security-related patterns within intricate traffic datasets. In addition, Xydas et al. studied three-dimensional graph visualization to help monitor the network for intrusion detection purposes, and discussed the importance of visualization to support security analysts' understanding of the network relationships between activity [26]. The results imply that accurate machine-learning predictions may not be enough; the findings should also be communicated in an understandable manner that allows administrators and security analysts to make swift decisions.

Moreover, it has been found that visualization and AI have been playing a crucial role in a variety of application fields[27]. The research trends of Artificial Intelligence were analysed, and systematic bibliometric and visual study of the research trends was conducted by Jia et al. [28] which highlights the growing significance of visualisation tools for gaining insight into complex research and technological developments. In addition, Wang and Zhan have applied visualization analysis to AI technologies, showing that visual analytical methods can help to grasp the understanding of large and complex information spaces [29]. These studies don't specifically focus on network-security monitoring but offer key evidence of the added value of visualization in AI-driven analytical systems.

Artificial intelligence is also more and more used in intelligent traffic-management and prediction systems. In the field of smart cities, Gheorghe and Soica [30] discussed the use of AI, IoT and predictive analytics[31] as tools to enhance adaptive traffic-control systems, underlining the power of intelligent and data-driven decision making[32] in dynamic environments. Rosca et al. showed an AI-based scheduling of public urban transport system and showed how an intelligent algorithm can be applied to optimize complex transport processes [33]. Ortner et al. presented an air-traffic-control system with built-in Artificial Intelligence that can predict collisions to highlight the possibility of an AI-based predictive system to assist in making

operational decisions in real-time [34]. These two studies are not strictly about cybersecurity, but they support the wider application of AI to monitoring, predicting and decision making in real time in the field of transportation.

Mohammed and Saleh summarize the artificial intelligence algorithms used for computer network traffic analysis in computer network research. The use of intelligent algorithms in classification, monitoring and analysis of traffic is increasingly expanding, they report [35]. Molina et al. proposed a real time traffic monitoring and visualization system that uses road side sensors, and demonstrated how the real-time sensing and visualization can be integrated to supply continuous traffic monitoring data [36]. Such studies highlight the need to consider data acquisition, automated analysis and visualization, as a unified process.

Even with all of these developments, recent studies have revealed that there is a lack of integration and effective integration of these AI-driven network monitoring systems that encompass real-time traffic collection, feature engineering, supervised traffic classification, unsupervised anomaly detection, and interactive visualization into a single operational system. In some areas like traffic classification, anomaly detection, prediction or visualization, existing works are plentiful. This will leave the network administrator needing to handle various methods of data collection, machine learning analysis and visual interpretation. This segmentation can exacerbate the complexity of operations and result in challenges in quickly making security decisions based on the AI generated results.

The shift from a packet-based to a scalable flow-based approach to network monitoring. Packet capture tools, like Wireshark and tcpdump, offer detailed visibility of packets, but as the number of packets grows, it becomes challenging to store and analyze all packets. Technologies like NetFlow, IPFIX and sFlow compact traffic into flows using flow identifiers and generate small flow records that include packet, byte and duration counts.

Deep Packet Inspection can be used to return a wealth of information on the payload and can be used to detect threats through signature.

But modern encryption makes the payload less visible and the deep inspection of high-speed links is a computation-intensive process. Another method, behavioral flow analysis, relies on packet headers, timing, rates and packet statistical properties, rather than decryption of the payload. Traditional machine learning algorithms used for intrusion detection are Naive Bayes, Decision Trees, K-Nearest Neighbors, Support Vector Machines, Random Forests and gradient-boosted tree algorithms. If a sufficient amount of labeled traffic exists, supervised approaches can achieve good performance. XGBoost is observed to be a good classifier for high dimensional network-flow data, which it can model the non-linear feature interaction and efficiently perform inference. The patterns that are labelled are the only ones that the supervised classification can operate on. In unsupervised approaches, the problem is tackled by learning the structure of normal traffic and identifying observations that fall outside of the learned representation. Classical anomaly-detection techniques consist of Isolation Forests and One-Class SVMs; Deep Autoencoders model compact behavior of normal networks. For the sequence of network data, recurrent neural network and LSTM networks can be useful. The reconstruction error can be used to detect anomalous traffic in an autoencoder. The thesis states that many studies concentrate on the accuracy of the model, but they don't really consider the needs of the Security Operations Center analysts. Even if the models are accurate, the size of uncontextualized logs, the lack of topology representation in logs, and the late arrival of alert interpretation can be of limited value.

Research Gap

- High computational overhead or offline-only evaluation in some existing approaches.
- Limited end-to-end treatment of packet/flow ingestion, feature engineering, AI inference, alert brokerage, and visualization.

Research Objectives

- Develop a scalable pipeline for extracting statistical properties from packet and NetFlow information.

- Develop a hybrid AI framework combining XGBoost for known-threat classification with a Deep Autoencoder for anomaly detection.
- Provide an interactive dashboard with real-time bandwidth statistics, topology visualization, protocol information, and alerts through WebSockets.

Methodology

The proposed system is organized as a four-tier pipeline: data ingestion, feature engineering and flow aggregation, hybrid AI analytics, and visualization and alert brokerage. The separation of these functions allows packet collection and preprocessing to operate independently from the machine-learning models and presentation layer.

Table 1: over of End-to-End Architecture

Tier	Main Function	Technologies Components	/
1. Data Ingestion	Collect live and historical traffic	Libpcap, Scapy, PyShark, NetFlow/IPFIX, PCAP	
2. Feature Engineering	Create bidirectional flows and 42-feature vectors	5-tuple grouping, temporal and statistical features	
3. AI Analytics	Known-threat classification and anomaly scoring	XGBoost + Deep Autoencoder	
4. Visualization	Stream results and present analyst views	FastAPI, WebSockets, React.js, D3.js, Recharts	

1.2 Data Ingestion and Flow Processing

The system supports live interface capture as well as offline PCAP and flow-log ingestion. Invalid or irrelevant frames are filtered, while TCP, UDP, and ICMP traffic proceeds to the analysis pipeline. Packets are grouped into bidirectional flows using the five-tuple representation. A flow ends when no packet is observed for more than 30 seconds or when a TCP FIN/RST termination is observed.

1.3 Feature Engineering

For every active flow, the system generates a vector of 42 statistical and temporal features. These include inter-arrival-time statistics, packet and byte rates, and packet-length distribution measures such as mean, standard deviation, minimum, maximum, and skewness.

1.4 Mathematical Formulation

We have z-score normalized features for a flow vector x : $x_scaled = (x - \mu)/\sigma$, where μ and σ are the mean and standard deviation of the training set of x . The Deep Autoencoder is trained to learn a reconstruction function $f(x)$ and the anomaly score is defined as the mean squared reconstruction error: $MSE = \frac{1}{n} \sum (x_i - \hat{x}_i)^2$

If the reconstruction error for a flow exceeds the anomaly threshold that was selected, the flow is seen as a potential previously unseen anomaly.

1.5 Hybrid AI Analytics Engine

1.5.1 XGBoost Supervised Classifier

The supervised branch uses XGBoost to classify known network conditions and attack categories. The selected configuration uses multi:softprob multi-class output, maximum tree depth of 8, learning rate of 0.05, 500 estimators, subsample ratio of 0.8, and colsample_bytree of 0.9. Grid search and multi-fold cross-validation were used during model development.

1.5.2 Deep Autoencoder

The unsupervised branch is a symmetric Deep Autoencoder implemented in PyTorch. It contains 42 input nodes, an encoder of 32, 16, and 8 nodes using ReLU activations, and a decoder of 16, 32, and 42 nodes with a linear output layer. Training uses Adam optimization with a learning rate of 0.001, batch size 256, 100 epochs, and mean squared error loss.

1.6 Consolidated Alert Payload

The two branches are side by side. Both XGBoost and the Autoencoder give an attack classification and a confidence score. These outputs are combined and form a single alert payload which contains the timestamp, source and destination information, classification, confidence, reconstruction loss and anomaly status.

1.7 Live Visualization

The FastAPI backend packages the results into

JSON and pushes them to the visualization layer over WebSockets, avoiding the need to repeatedly poll for updates. The interface is built with React.js and D3.js, and displays ongoing connectivity and traffic levels graphs, interactive graph topologies and an ongoing alert feed. Under threat nodes and links are visually highlighted and alert cards display the source and destination addresses, type of attack detected, model confidence and anomaly score.

Table 2: Experimental Environment

Component	Specification
Operating System	Ubuntu 22.04 LTS, Linux Kernel 5.15 with PREEMPT_RT
CPU	Intel Core i9-14900K, 24 cores / 32 threads
Memory	64 GB DDR5 RAM, 5600 MHz
GPU	NVIDIA GeForce RTX 4090, 24 GB VRAM
Storage	2 TB NVMe PCIe 4.0 SSD
Programming	Python 3.10.12
ML/DL	Scikit-Learn 1.3.2, XGBoost 2.0.3, PyTorch 2.1.2
API / Streaming	FastAPI 0.109.0, Uvicorn, Native WebSockets
Frontend	React.js 18.2, Tailwind CSS, D3.js, Recharts

2. Dataset and Experimental Setup**Table 3: Attack Categories**

Category	Examples / Description
DDoS / Flooding	LOIC and HOIC traffic
DoS	Slowloris, Slowhttptest, Hulk, Goldeneye
Brute Force	SSH and FTP credential attacks
Web Attacks	SQL injection, XSS, brute-force web logins
Infiltration	External payloads leading to internal compromise
Botnet	Zeus and Ares command-and-control traffic
Port Scanning	Scanning of open ports and services

2.1 Preprocessing of data

- Cleaning: Drop rows containing NaN or infinite values, and drop corrupt header.

Feature Scaling: An alternative is to normalize the feature values using z-scores so that large scale measurements do not overwhelm small timing features.

- Class balancing: Only use for training set. SMOTE is applied to boost minority class of attacks.

Data split: 70/15/15 (training/validation/Final test).

2.2 Real Time Stress Testing

The PCAP traffic is fed into the processing pipeline at various rates by a Python-based traffic replay mechanism and distribution delay and processing time from intake to inference are observed. Evaluation Metrics

The evaluation uses the following standard measures:

- Accuracy = $(TP + TN) / (TP + TN + FP + FN)$
- Precision = $TP / (TP + FP)$
- Recall = $TP / (TP + FN)$
- F1-score = $2 \times (Precision \times Recall) /$

(Precision + Recall)

3. Results

Two classifiers (the proposed supervised XGBoost classifier and unsupervised Deep Autoencoder) were tested and benchmarked against three baseline classifiers (Logistic

Regression, Support Vector Machine and Random Forest). The results reported in the thesis show that XGBoost has the strongest overall classification performance while the Autoencoder provides a complementary capability for anomalous behavior.

Table 5 : Comparative Machine-Learning Performance

Model	Accuracy %	Precision %	Recall %	F1 %	Training s	Latency ms/flow
Logistic Regression	88.42	86.10	87.30	86.69	12.4	0.4
SVM	93.15	92.80	91.40	92.09	1,420.0	14.2
Random Forest	99.31	99.20	99.35	99.27	184.0	2.8
XGBoost	99.45	99.50	99.40	99.45	92.0	1.8
Deep Autoencoder	96.80	95.10	97.20	96.14	340.0	3.2

3.1 Interpretation of Model Results

Logistic Regression has the lowest classification accuracy with the highest inference latency of the evaluated models due to the network-flow relationships that result in the inference latency. Random Forest shows good performance and XGBoost is the best reported overall supervised performance with 99.45%

accuracy and F1-score and 1.8 ms inference latency per flow.

The accuracy of the Deep Autoencoder was 96.80% and F1 score was 96.14%. The proposed system does not aim at replacing XGBoost but to use it as an additional unsupervised anomaly signal for traffic patterns which are not defined by the supervised labels.

Table 6: Attack-Specific Detection

Attack Category	Precision %	Recall %	F1 %	Test Samples
Benign	99.84	99.78	99.81	1,000,000
DDoS (LOIC/HOIC)	99.95	99.98	99.96	150,000
DoS (Slowloris/Hulk)	98.70	98.10	98.40	20,000
Web Attacks (SQLi/XSS)	96.40	95.20	95.80	5,000
Botnet Communication	99.10	98.80	98.95	12,000
Infiltration	94.20	92.60	93.39	3,000

A security monitoring platform doesn't just have to be accurate when it comes to classification. The processing delay may be too high and may make an intrusion-detection system not to work as a real-time defense mechanism. The thesis thus

Table 7: Latency, Throughput, and Scalability

Processing Component	Reported Average
Feature extraction	0.9 ms per packet batch
XGBoost inference	1.8 ms per flow vector
Deep Autoencoder reconstruction	3.2 ms per flow vector

WebSocket dashboard broadcast	1.1 ms transmission overhead
-------------------------------	------------------------------

5. Discussion

The experimental results indicate the importance of two complementary AI mechanisms that were adopted as the main design decision. XGBoost is a suitable algorithm for the classification of known traffic types to high accuracy because it is a nonlinear algorithm, thus it extends the monitoring pipeline beyond the closed set of supervised labels.

The best results for attack-specific detection are found in high-volume DDoS and botnet traffic in which the statistical properties of the traffic are very distinguishable, and in which the classification is not as complicated. As the attacks and infiltration on the web are both

subtle and less frequent, their recall and precision are relatively less. From these results, it is recommended that future improvements be focused on challenging application-oriented attack behavior in particular, which occurs at low volume.

5.1 Relevance for Operations

Thus, the task of this work is more than just an accuracy score. The whole pipeline is: traffic collection, feature extraction, AI inference, alert generation and visualization. This allows analysts in a SOC to rapidly understand the output of AI, rather than reading through tons of raw logs.

6. Comparative Analysis and Practical Implications

Table 8: Comparison with Existing Work

Reference / Work	Main Approach	Dataset	Reported Result	Operational Gap
Sharafaldin et al. (2018)	Random Forest, KNN	CIC-IDS-2017	96.50% detection rate	Offline evaluation; no real-time stream pipeline
Wang et al. (2021)	1D-CNN + Autoencoder	UNSW-NB15	97.80% F1	High inference overhead; no visualization dashboard
Dhakad et al. (2023)	Random Forest, XGBoost	Custom NetFlow	99.31% accuracy	Classification focus; no zero-day anomaly scoring
Zhang et al. (2024)	Deep Autoencoder	CIC-IDS-2018	95.40% anomaly recall	No supervised multi-vector categorization
Proposed work	XGBoost + Autoencoder + WebSockets UI	CIC-IDS-2018 + live stream	99.45% accuracy; 3.2 ms anomaly latency	Integrated end-to-end monitoring and visualization

5.1 Practical Implication

Enterprise network monitoring: The system can turn out of the way high volume flow information into digestible and machine-readable security events.

Security Operations Centers - The live dashboard can help to decrease manual correlation of raw logs and can display alerts that include contextual information about the source, destination, confidence and anomaly.

Access to encrypted traffic environments: The feature-engineering approach uses flow

statistics instead of payload. Supervised and Unsupervised signals could be used together for Incident response for known-attack classification, and for other anomaly evidence. Scalable monitoring research: modular structure makes future replacement or extension of the feature-engineering and AI components easier.

5.2 Suggested Applications

Be used as a complement to other security measures, rather than a replacement for them

all. It can supplement current network monitoring and IDS environment with behavioral analytics, anomaly scoring and analyst friendly visual interface.

7. Limitations and Future Work

7.1 Constraints

There are several limitations to the thesis. Supervised models (such as XGBoost) first require representative labeled data for training. Second, if the attackers can do it deliberately or introduce a small amount of false traffic to go under the detection threshold, even high-performing classifiers and autoencoders can be evaded. The learning outcomes in this evaluation are based on CIC-IDS-2018 and simulated / live replay conditions and are therefore presented as 5.2 Future Research Directions.

- Explore the federated learning techniques that can be used to allow multiple organizations to cooperate with each other without sending raw network traffic.

Use Graph Neural Networks to replace or augment the existing feature-engineering phase, to capture relationships between hosts, routers and internal communication paths.

Test in more real-world traffic sources and large deployments in the operational network.

- representations.

Understand explainable AI techniques to help security analysts gain insights into the important characteristics of a classification or anomaly score.

Improve the visualization components and add in more topology analyses, alerts and analyst feedback loops.

Evaluate resistance to traffic timing and feature distributions adversarial attacks.

Each policy and operations recommendation is marked with a number. Each policy and operations recommendation is numbered.

Integrated with current working practices. Models should be retrained based on guidance provided by controlled data-quality processes and alert thresholds should be reviewed with traffic behavior changes. But organisations must implement their own Rules of Data Retention, Rules of Access and Rules of Monitoring to the proposed pipeline.

Phased deployment of the operational feature pipeline: validate the feature pipeline with

representative traffic; deploy the AI system in observation mode; add high-confidence alerts to the incident response workflow; add automated actions after adequate validation and governance.

8. Conclusion

This paper presented an AI-based network traffic monitoring and visualization system that addresses the ingestion, 42 feature statistical representation, supervised XGBoost classification, unsupervised Deep Autoencoder anomaly detection and a real time WebSocket based visualization interface.

The classification performance of the evaluation in the underlying thesis is desirable. XGBoost's accuracy was 99.45%, precision 99.50%, recall 99.40% and F1-score 99.45% with an inference latency of 1.8ms per flow. The accuracy of Deep Autoencoder was 96.80% and F1-score was 96.14%. It offers a complementary anomaly detection signal for traffic which is not part of any known supervised category. The evaluation performed in the attack-specific case revealed that the performance was good for DDoS and botnet attacks, but was harder to achieve when it came to web attacks and infiltration.

The reported experiments require only a millisecond for model inference, anomaly reconstruction and WebSocket delivery. The dashboard translates model outputs into network topology, time-series, and alert views to help Security Operations Center analysts. The thesis claims that during simulated incident-response drills, the identification of attack source, vector and scope is six times faster than traditional CLI-based log review.

Overall, the results are in favor of using a hybrid supervised and unsupervised AI pipeline for network monitoring. The work is not an alternative to security controls, but rather a layer of intelligence and analytics with visual components that can be used to augment security monitoring, prioritization and incident response processes. Future validation on real world deployments, wider datasets, adversarial conditions and graph.

REFERENCES

- Ahmad, I., Nasim, F., Khawaja, M.F., Naqvi, S.A.A. and Khan, H., 2025. Enhancing IoT security and services based on generative artificial intelligence techniques: a systematic analysis based on emerging threats, challenges and future directions. *Spectrum of engineering sciences*, pp.1-25.
- Sadique, A., Sehar, H., Nasim, S. and Nasim, F., 2025. Data exposure risks in hybrid vs. multi-cloud migrations: a comparative analysis. *Journal of Applied Linguistics and TESOL (JALT)*, 8(1), pp.213-224.
- Ahmed, H.M.M., Bhatti, S.M. and Nasim, F., 2024. Object Identification for Autonomous Vehicles using Machine Learning. *Journal of Computing & Biomedical Informatics*, 7(01), pp.364-376.
- Jamal, A., Akbar, Z., Akbar, S., Niaz, S. and Tauseef, F., 2024. Detecting governance risk in generative AI adoption: a predictive analysis of organizational misalignment and AI failure signals. *Metallurgical and Materials Engineering*, 30(2), pp.122-140. Available at: <https://doi.org/10.63278/mme.v30i2.1965>.
- Ahona, M.H., Jamal, A., Tauseef, F., Mahmud, M. and Indika, M.H., 2026. AI-driven discovery of novel biomarkers for early cardiovascular disease detection. *Well Testing Journal*, 35(S2), pp.1-46. Available at: <https://doi.org/10.66669/WT.v35iS2.287>.
- Jamal, A., Akbar, Z., Akbar, S., Niaz, S. and Tauseef, F., 2022. Predicting human-GenAI collaboration effectiveness: a machine learning investigation of skill configurations, trust, and work design. *Migration Letters*, 19(S8), pp.2303-2324. Available at: <https://migrationletters.com/index.php/ml/article/view/12298>.
- Jamal, A., Tauseef, F., Naseer, F., Akbar, A., Jabeen, M. and Nasim, F., 2025. A convolutional neural network approach for diabetic retinopathy detection from retinal images: a critical review of deep learning techniques in ophthalmic diagnosis. *Multidisciplinary Surgical Research Annals*, 3(4), pp.3100-3128. Available at: <https://doi.org/10.5281/zenodo.20587510>.
- Ji, S.Y., Jeong, B.K. and Jeong, D.H., 2021. Evaluating visualization approaches to detect abnormal activities in network traffic data. *International Journal of Information Security*, 20(3), pp.331-345.
- Ball, R., Fink, G.A. and North, C., 2004. Home-centric visualization of network traffic for security administration. In: *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security (VizSEC '04)*. Washington, D.C., USA, 29 October 2004. New York: ACM, pp.55-64. Available at: <https://doi.org/10.1145/1029208.1029218>.
- Gheorghe, C. and Soica, A., 2025. Revolutionizing urban mobility: a systematic review of AI, IoT, and predictive analytics in adaptive traffic control systems for road networks. *Electronics*, 14(4), p.719. Available at: <https://doi.org/10.3390/electronics14040719>.
- Devadhas Sujakumari, P. and Dassan, P., 2023. Generative Adversarial Networks (GAN) and HDFS-based realtime traffic forecasting system using CCTV surveillance. *Symmetry*, 15(4), p.779. Available at: <https://doi.org/10.3390/sym15040779>.

- A. Jaramillo-Alcazar, J. Govea, and W. Villegas-Ch, "Advances in the Optimization of Vehicular Traffic in Smart Cities: Integration of Blockchain and Computer Vision for Sustainable Mobility," *Sustainability* (Switzerland), vol. 15, no. 22, Nov. 2023, doi: 10.3390/su152215736.
- Q. N. Naveed, H. Alqahtani, R. U. Khan, S. Almakdi, M. Alshehri, and M. A. A. Rasheed, "An Intelligent Traffic Surveillance System Using Integrated Wireless Sensor Network and Improved Phase Timing Optimization," *Sensors*, vol. 22, no. 9, May 2022, doi: 10.3390/s22093333.
- Bustamante-Bello, R., Garcia-Barba, A., Arce-Saenz, L.A., Curiel-Ramirez, A.A., Izquierdo-Reyes, J. and Ramirez-Mendoza, R.A., 2022. Visualizing street pavement anomalies through fog computing V2I networks and machine learning. *Sensors*, 22(2), p.456. Available at: <https://doi.org/10.3390/s22020456>.
- Ahmad, J., Tauseef, F. and Akbar, Z., 2024. Predictive analytics for AI-assisted patient no-show management and clinic revenue optimization: a simulation-based research. *Migration Letters*, 21(S13), pp.1901-1924.
- Jamal, A., Tauseef, F., Akbar, Z. and Niaz, S., 2023. Business intelligence in healthcare management: leveraging data analytics to improve strategic planning and organizational performance in hospitals. *Frontier in Medical and Health Research*, 1(1), pp.46-58. Available at: <https://fmhr.net/index.php/fmhr/article/view/2766>.
- Salau, A.O. and Beyene, M.M., 2024. Software defined networking based network traffic classification using machine learning techniques. *Scientific Reports*, 14(1), p.20060. Available at: <https://doi.org/10.1038/s41598-024-70983-6>.
- Nasim, M.F., Masood, S., Jaffar, A., Ahmad, U. and Rashid, M., 2025. Acoustic signal-based intelligent automotive engine failure detection and analysis system. *IEEE Access*, 13, pp.1-15. Available at: <https://doi.org/10.1109/ACCESS.2025.3524100>.
- Dhakad, A., Singh, S., Mohana, Moharir, M. and Ashok Kumar, A.R., 2023. Real time network traffic analysis using artificial intelligence, machine learning and deep learning: a review of methods, tools and applications. In: 2023 International Conference on Smart Systems and Advanced Computing (ICSSAS). Intent, India, 15-16 September 2023. IEEE, pp.372-378. Available at: <https://doi.org/10.1109/ICSSAS57918.2023.10331855>.
- Jamal, A., Tauseef, F. and Naseer, F., 2025. AI in digital healthcare transformation: analysing the impact of AI technologies on healthcare service delivery and operational efficiency. *The Research of Medical Science Review*, 3(12), pp.1530-1542. Available at: <https://medicalsciencereview.com/index.php/Journal/article/view/3716>.
- Akshatha, V. and Srinivasan, V., 2023. Artificial intelligence based network traffic analysis to handle large-scale and high speed traffic. *International Journal of Engineering Research & Technology (IJERT)*, 11(06), pp.1-4. Available at: <https://doi.org/10.17577/NCRTCA-PID-076>.
- Priya, V., 2024. Advancements in anomaly detection techniques in network traffic: the role of artificial intelligence and machine learning. *Journal of Scientific Research and Technology (JSRT)*, 2(3), pp.214-220. Available at: <https://doi.org/10.61359/2.2024.0321>.
- Mehdi, M., Nasim, F. and Munir, M.Q., 2024. Comparative risk analysis and price prediction of corporate shares using deep learning models like LSTM and machine learning models. *Journal of*

- Computing & Biomedical Informatics, 7(02). Available at: <https://jcbi.org/index.php/jcbi/article/view/178>.
- Kapadia, M., Dunton, A., Jaculina, C., Thach, D., Ong, A. and Chang, S.Y., 2025. Data visualization and preprocessing for network traffic analysis in cybersecurity. arXiv preprint arXiv:2501.12345 [or specify publisher/journal name]. Available at: <https://doi.org/10.48550/arXiv.2501.12345>.
- Jamal, A., Naseer, F., Akbar, S. and Tauseef, F., 2024. Business analytics in the GenAI era: a systematic review of value pathways, failure modes, and governance mechanisms. *Journal of Innovative Computing and Emerging Technologies*, 4(1). Available at: <https://jicet.org/index.php/JICET/article/view/246>.
- Xydas, I., Miaoulis, G., Bonnefoi, P.F., Plemenos, D. and Ghazanfarpour, D., 2005. 3D graph visualization prototype system for intrusion detection: a surveillance aid to security analysts. In: *Proceedings of the International Conference on Computer Graphics and Artificial Intelligence (3IA)*. Limoges, France, May 2005, pp.1-10.
- Tauseef, F., Jamal, A. and Naseer, F., 2023. Artificial intelligence in healthcare systems exploring the transformational role of AI technologies in healthcare management and clinical decision support. *Review Journal of Neurological & Medical Sciences*. Available at: <https://doi.org/10.5281/zenodo.20023513>.
- Jia, Q., Wang, X., Zhou, R., Ma, B., Fei, F. and Han, H., 2023. Systematic bibliometric and visualized analysis of research hotspots and trends in artificial intelligence in autism spectrum disorder. *Frontiers in Neuroinformatics*, 17, p.1310400. Available at: <https://doi.org/10.3389/fninf.2023.1310400>.
- Wang, J. and Zhan, Q., 2021. Visualization analysis of artificial intelligence technology in higher education based on SSCI and SCI journals from 2009 to 2019. *International Journal of Emerging Technologies in Learning (iJET)*, 16(8), pp.20-33. Available at: <https://doi.org/10.3991/ijet.v16i08.18447>.
- Gheorghe, C. and Soica, A., 2025. Revolutionizing urban mobility: a systematic review of AI, IoT, and predictive analytics in adaptive traffic control systems for road networks. *Electronics*, 14(4), p.719. Available at: <https://doi.org/10.3390/electronics14040719>.
- Jamal, A., Tauseef, F., Naseer, F., Akbar, A. and Jabeen, M., 2025. Predictive AI healthcare analytics for early disease detection leveraging AI and machine learning models to identify high-risk patients and improve preventive healthcare strategies. *Annual Methodological Archive Research Review*, 3(11), pp.1-28. Available at: <https://doi.org/10.5281/zenodo.20686563>.
- Nasim, F., Yousaf, M.A., Masood, S., Jaffar, A. and Rashid, M., 2023. Data-driven probabilistic system for batsman performance prediction in a cricket match. *Intelligent Automation & Soft Computing*, 36(3), pp.3211-3226. Available at: <https://doi.org/10.32604/iasc.2023.034567>.
- Rosca, C.M., Stancu, A., Neculaiu, C.F. and Gortoescu, I.A., 2024. Designing and implementing a public urban transport scheduling system based on artificial intelligence for smart cities. *Applied Sciences*, 14(19), p.8861. Available at: <https://doi.org/10.3390/app14198861>.
- Ortner, P., Steinhöfler, R., Leitgeb, E. and Flühr, H., 2022. Augmented air traffic control system—artificial intelligence as digital assistance system to predict air traffic conflicts. *AI*, 3(3), pp.623-644. Available at: <https://doi.org/10.3390/ai3030036>.

Mohammed, O.Y. and Saleh, I.A., 2024. Survey of computer network traffic analysis using artificial intelligence algorithms. *International Research Journal of Innovations in Engineering and Technology*, 8(12), pp.11-19. Available at: <https://doi.org/10.47001/irjiet/2024.812002>.

Molina, J.M.G., Sotis, A.S., Pascual, R.C., Cubillas, J.E.D. and Matias, J.B., 2022. Development of real-time traffic monitoring and visualization system using stationary roadside sensor. In: *Proceedings of the 2022 5th International Conference on Algorithms, Computing and Artificial Intelligence (ACAI '22)*. Sanya, China, 23-25 December 2022. New York: Association for Computing Machinery, pp.154-160. Available at: <https://doi.org/10.1145/3579895.3579919>.

