IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 6, June 2025

DOI: 10.17148/IARJSET.2025.12649

# Networking with AI: Optimizing Network Planning, Management, and Security through the medium of Artificial Intelligence

**Naveed Uddin Mohammed[1], Zubair Ahmed Mohammed[2], Shravan Kumar Reddy Gunda[3], Akheel Mohammed[4], Moin Uddin Khaja[5]**

School of Computer and Information Science, Lindsey Wilson College, KY, USA[1,2,5]

Department of Information Technology, Northwestern Polytechnic University, CA, USA[3]

School of Computer and Information Science, University of the Cumberlands, KY, USA[4]

**Abstract:** Greater complexity in current computer networks, introduced in response to cloud computing, Internet of Things (IoT), and 5G technologies, has made complex approaches towards managing, optimizing, and securing network systems prominent. The traditional network management techniques, rooted primarily in strict rules and human intervention, are unable to cope with the amount of data and dynamics of current networks. Therefore, the use of Artificial Intelligence (AI) in networking is becoming a game-changer. Artificial Intelligence (AI) through such technologies as machine learning (ML), deep learning (DL), reinforcement learning (RL), and natural language processing (NLP) can indeed assist in enhancing the design, management, and security of the network system. There are a number of ways by which AI can optimize the networks. Traffic patterns for smart traffic control as well as resource allocation can be forecast using machine learning algorithms. The anomaly detection capabilities of machine learning-based systems also provide real-time security attack detection, hence mitigating the impact of attack vectors such as Distributed Denial of Service (DDoS) or malware attacks. Lastly but not the least, AI is capable of offering self-healing networks that automatically detect faults and heal themselves as required without human intervention, a business of unimaginable value in enormous systems. Reinforcement learning is very beneficial for dynamic routing and load balancing through constant adjustment of network parameters to changing conditions. Other applications of AI in the networks include optimization of Quality of Service (QoS), where applications with high priority such as video streaming or gaming are assigned the bandwidth, they require to function efficiently. In addition, with edge computing and 5G networks, the work of AI is ensuring that network resources are optimally distributed to edge devices for maximum scalability and performance. However, there are some limitations in the use of AI for networking. It needs to be extensively tested with data privacy issues, interpretability of the model, and computational complexity of the AI model. The requirement for high real-time performance puts constraints in processing the network, which can be itself a limiting factor for the use of AI in some applications. Even with these challenges, the potential of AI to revolutionize networking cannot be overstated, and work on network systems with AI at its foundation will probably yield more intelligent, more autonomous, and more secure networking choices.

**Keywords:** Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL), Reinforcement Learning (RL), Natural Language Processing (NLP), Network Management, Traffic Optimization, Anomaly Detection, Self-healing Networks, Network Security, Distributed Denial of Service (DDoS), Quality of Service (QoS), Edge Computing, 5G Networks, Autonomous Networks, Network Optimization, Real-time Performance.

## I. INTRODUCTION

The pace of digital transformation has picked up pace in various sectors, so the need for more efficient, reliable, and secure computer networking infrastructure is never greater [1]. With the Internet of Things (IoT), cloud, and 5G technologies evolving exponentially, the level of computer networking manageability, optimization, and security has never been more challenging to attain. The traditional network management methods based on primarily human intelligence, manual adjustment, and static configuration are not capable of handling the volume of data produced by such sophisticated network environments. Secondly, real-time decision-making and dynamic response to dynamic network environments is not something that traditional systems can offer.

Artificial Intelligence (AI) is also developing as an extremely useful tool to deal with such occurrences [2]. AI engages a series of methods such as machine learning (ML), deep learning (DL), reinforcement learning (RL), and natural

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 6, June 2025

DOI: 10.17148/IARJSET.2025.12649

language processing (NLP) to mention a few, which may be utilized in an attempt to take advantage while automating, enhancing, and securing network infrastructure [3]. The power of AI in dealing and managing humongous data in real-time has ghastly benefits over conventional network approaches since AI allows one to achieve highly responsive, highly scalable, and highly efficient networks.

Automation is the best means by which AI will revolutionize networking. Network administrators, in traditional networks, will do things manually, keep equipment online, watch over their performance, and defend against security weaknesses. But through AI, all these are automatically addressed without any human intervention and made network management easier to do. Machine learning applications, for example, can be utilized to predict network traffic patterns and routing decisions in real-time, offering the best performance without any intervention of human beings [4]. It's such a level of automation that's being used at network fault detection and healing so that the AI environment can detect faults in the network, fault diagnosis, and healing fault autonomously.

AI also plays an important role at security for the network. Whereas the threats at cyberspace are becoming even more sophisticated nowadays, the old security measures do not have any ability to identify and ward off the attacks at real-time. AI-based anomaly products can observe network traffic and identify anomalous behavioural patterns, allowing for quick identification of potential security threats. Deep learning algorithms also have the capability to enhance intrusion detection systems' (IDS) performance by constantly learning from emerging attack patterns, thus enhancing their ability to defend against emerging attacks [5].

Besides automation and security, AI also improves network optimization through dynamic resource management, Quality of Service (QoS) management, and load balancing. AI provides improved traffic management through consideration of real-time instantaneous network measurements, directing mission-critical applications to the right resources while limiting network usage.

With 5G and edge computing, networks will become more complex, and the role of AI will be more critical than ever [6]. Edge processing on-premises and responding to changing network conditions will become essential for enabling next-generation autonomous, cognitive networks.

## II. AI NETWORKING TECHNIQUES

Artificial Intelligence (AI) networking adoption relies on a group of basic systems learning techniques, environmental adaptation, and self-governing decision making. They are Machine Learning (ML), Deep Learning (DL), Reinforcement Learning (RL), and Natural Language Processing (NLP) and have the same functionalities of intelligence amplification and automating existing networks [7].

### 2.1. Machine Learning (ML)

Machine Learning is the most basic AI technique used in networking. ML is where historical network data is learned from in the form of patterns to predict or make decisions without being programmed beforehand [8]. In network usage, ML can be applied in traffic classification, traffic congestion prediction, bandwidth allocation, and anomaly detection. For instance, supervised ML algorithms can be employed to classify network traffic types, while unsupervised ML detects behaviour anomalies that could potentially signify security threats or misconfiguration. ML is also used for network performance forecasting and hardware predictive maintenance to forecast potential future chokepoints.

### 2.2. Deep Learning (DL)

Deep Learning is an ML method that makes use of artificial neural networks with more than one layer to map complex high-dimensional relationships in the data [9]. DL is used best on unstructured network data such as packet payloads, logs, and telemetry.

Deep learning networks like Recurrent Neural Networks (RNNs) and Convolutional Neural Networks (CNNs) in cyber security are able to detect sophisticated or advanced malware or advanced persistent threats (APTs) by detecting complex patterns of data that might be overlooked using signature-based mechanisms [10]. DL further facilitates application-aware network traffic inspection to re-distribute resources as per actual utilization patterns.

### 2.3. Reinforcement Learning (RL)

Reinforcement Learning is a learning process where an agent takes an action on an environment, decides something, and gets rewarded or punished accordingly [11]. RL has its most valuable applications in networking where the decision-making needs to vary dynamically based on varying situations. Dynamic routing, load balancing, and wireless spectrum management are a few of them. RL-based methodologies, i.e., Q-learning and Deep Q-Networks (DQNs), are trainable to fine-tune route in terms of current latency and congestion as parameters for better Quality of Service (QoS) and utilization of network resources.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 6, June 2025

DOI: 10.17148/IARJSET.2025.12649

### 2.4. Natural Language Processing (NLP)

Human language can be utilized by computers so that the latter can grasp and convey because of Natural Language Processing. NLP is increasingly being deployed in network architecture as part of automated network networks where administrators enter parameters, interrogate network conditions, or answer in natural language [12]. Virtual assistant and chat agents empowered with NLP facilitate the maintenance of networks through simpler interaction platforms, especially needed in very networked multisource deployments where multiple vendors need to be maintained and well worth it. NLP also facilitates parsing and analysis out of logs and documents to provide actionable information.

All these AI techniques combined are shaping the future of networking by automating, adapting, and intelligent Ing the equipment.

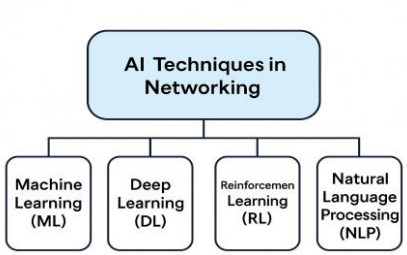


Figure 1: AI Techniques in Networking

## III. AI APPLICATIONS IN NETWORKING

Artificial Intelligence has been utilized in a wide range of networking fields, enabling network management, security, and optimization to a very great extent. The current networks are more flexible, self-governed, and decision-making due to AI techniques [13]. Some of the most significant implementation areas where AI has the main responsibility are as follows:

### 3.1. Traffic Management

AI is also extensively used in dynamically and intelligently managing traffic within the network [14]. Reinforcement learning and machine learning allow networks to predict traffic patterns, identify bottleneck locations, and reroute data through best paths. This reduces latency and enhances throughput. Adaptive traffic management also provides better bandwidth utilization and user experience, particularly in applications with high demand like data centers or city 5G networks.

### 3.2. Network Security

AI transformed network security through the ability to detect and prevent threats in real time [15]. Deep learning and anomaly detection technology has the capability to analyse gigantor amounts of traffic data for malicious patterns, identify zero-day attacks, and prevent intrusions. AI-powered IDS and firewalls ensure dynamic protection by learning about new cyber threats on the fly.

### 3.3. Fault Detection and Recovery

Self-healing networks are now possible with the assistance of fault detection with AI [16]. They utilize machine learning and deep learning to monitor devices in the network, identify diminishing performance, and identify cause of failure. Automated recovery procedures can be triggered upon detection to reduce downtime and ensure network stability without the involvement of a human operator.

### 3.4. Quality of Service (QoS) Optimization

AI offers mission-critical functions like video conferencing, VoIP, or online gaming with the capabilities to carry it out well. Dynamic allocation of bandwidth, packet prioritization, and AI-based real-time monitoring ensure smooth operation for high-priority services [17]. Agents based on reinforcement learning continue to learn from usage contexts to uphold desired service levels.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 6, June 2025

DOI: 10.17148/IARJSET.2025.12649

Table 1: Summary of AI Applications in Networking

| Application | AI Technique Used | Benefits |
|---|---|---|
| Network Automation | 85 | 90 |
| Security & Threat Detection | 75 | 85 |
| Predictive Maintenance | 65 | 80 |
| Traffic Management | 70 | 75 |
| Customer Support | 60 | 70 |

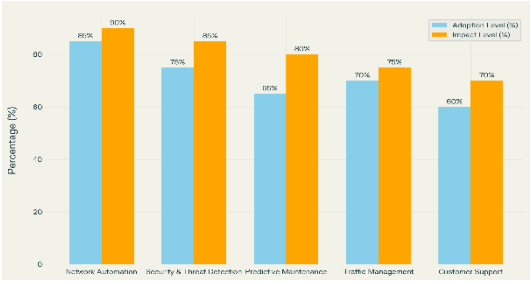


Figure 2: AI Applications in Networking (Adoption/Impact Levels)

## IV. CASE STUDIES: REAL-WORLD APPLICATIONS OF AI FOR NETWORKING

Several top technology companies have shown the real-world application of Artificial Intelligence for networking [18]. The case studies show how AI enhances performance, reliability, and security in complex network infrastructures.

### 4.1. Google's B4 Network: AI for Traffic Engineering

Google's B4 is an internally developed software-defined WAN (Wide Area Network) linking its data centers worldwide [19]. Google applies machine learning and AI to dynamically optimize network traffic engineering. By examining historic and projected traffic demand, the AI platform performs dynamic routing decision adjustments to optimize bandwidth usage and avoid congestion. As a result, B4 had over 90% link utilization with maintaining high reliability and low latency. This case illustrates the ability of AI to attain unprecedented scalability with minimal human intervention.

### 4.2. Cisco AI Network Analytics: Predictive and Proactive Maintenance

Cisco has infused AI into network monitoring to anticipate device failure and perform proactive maintenance [20]. Its AI analytics platform based on machine learning analyses device performance and user activity in real-time to find anomalies. It warns administrators in advance of a performance slowdown or outage. AI-driven insights have cut problem-solving time by as much as 35% and customer satisfaction by ensuring quality delivery of services [21]. This is just one example of how efficiency and reliability of operations are boosted with the use of AI.

### 4.3. Facebook NetNORAD: Fault Detection AI

Facebook developed NetNORAD, an AI-powered tool for detecting network failures independent of device telemetry [22]. Instead of relying on hardware alerts, NetNORAD sends probe packets and uses AI to analyse path-level performance across the network. It identifies disruptions even when devices report normal status, uncovering hidden failures. NetNORAD has significantly improved Facebook's ability to diagnose complex issues across its global infrastructure. This case illustrates AI's capacity for deep, data-driven fault detection in hyperscale networks.

### Summary of Adoption Trends

These organizations are the pioneers as far as AI networking is concerned [23]. The rates of adoption have continually improved over time owing to the awareness of the fact that AI has been the cornerstone when it comes to performance, security, and automation.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 6, June 2025

DOI: 10.17148/IARJSET.2025.12649

## V. BENEFITS OF AI IN NETWORKING

Artificial Intelligence (AI) application in network technologies has revolutionized the operation of contemporary networks into smart, responsive, and much more efficient [24]. The below are the key advantages of AI implementation in networking, categorized by effect areas:

### 5.1. Simplifying routine and repetitive tasks

AI is superb at simplifying routine and time-consuming network operations, including configuration management, performance monitoring, and firmware updates [25]. AI minimizes the amount of human touch, human error, and delivers uniformity through intelligent automation. AI-based solutions help network administrators automate tedious processes like dynamic routing updates or patches, allowing IT specialists to dedicate more time to strategic work. Shifting from manual to automated operations improves network management responsiveness by a significant margin.

### 5.2. More Efficient Network

AI improves network performance in general by routing traffic, loads, and bandwidth use [26]. Through examination of history along with real-time data, machine learning and predictive analytics can inspect traffic patterns for predictions and avoid traffic congestion. For instance, AI will route packets on less busy routes to enable data to travel without significant delay. All this intelligent decision-making gives a better user experience, particularly in high-traffic environments such as cloud operations or IoT deployments [27].

### 5.3. Security Posture Enhanced

Security solutions based on artificial intelligence are important to identify and remove threats in no time 28[]. Rule-based and static security solutions are traditional, which cannot identify today's cyber-attacks. AI utilizes the deep learning, anomaly detection, and behaviour analysis models to identify abnormal behaviour like data breaches, malware attack, or Distributed Denial of Service (DDoS) attacks [29]. Deep learning allows the identification of concealed patterns, and behaviour analysis supports the identification of unknown threat without depending on signatures. The systems remain in learning mode all the time and improve continuously on a permanent basis, delivering proactive defence features that minimize the likelihood of security attack and loss of data [30].

### 5.4. Minimize Operations Costs

By minimizing human effort, minimizing downtime, and optimizing use of resources, AI minimizes the cost of operations [31]. Predictive maintenance and auto-healing features minimize emergency response and optimize network hardware life cycle. In large environments, automation through AI can be efficient in handling thousands of network devices compared to manual techniques, saving organizations considerable financial and human capital [32].

Briefly, AI turns networking into an intelligent, proactive network rather than an intelligent, human-directed system. Cisco automation, efficiency, security, and cost savings not only optimize the performance of the network but also enable organizations to future-proof for scalability and future technology advances.

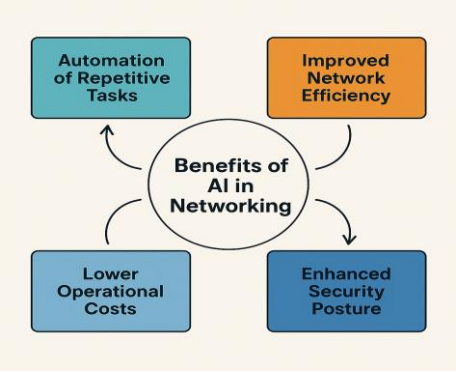


Figure 3: Benefits of AI in Networking

## VI. CHALLENGES AND RISKS OF AI IN NETWORKING

Artificial Intelligence (AI) has tremendous potential to provide in the domain of networking but also comes with some challenges and risks that have to be dealt with to implement secure and sustainable implementation [33]. Those challenges range from technical and operational to ethical and regulatory. It is very much necessary to familiarize oneself with such challenges for implementation [34].

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 6, June 2025

DOI: 10.17148/IARJSET.2025.12649

### 6.1. Data Privacy and Security

Perhaps the most urgent matter is protecting the enormity of information that is dealt with by AI systems. Networked AI depends to a great extent on the gathering and processing of user and system information in order to operate effectively [35]. This can be a privacy issue, however, when there is sensitive or personally identifiable information (PII) at stake [36]. AI systems would remain vulnerable to cyber-attack or unwittingly spill confidential information unless effectively managed. The implementation of strong encryption, data anonymization, and regulation like GDPR is imperative.

### 6.2. Insufficient Trained Manpower

AI networking is a specialized occupation that requires network engineers not just to possess machine learning and data science skills but also industry experience in them [37]. Professional lack of ability with inter-disciplinary knowledge hinders adoption and inhibits innovation. Firms may find it difficult to identify or re-skill capabilities to develop and maintain AI-driven network infrastructure [38]. The aforementioned capability gap calls for investment in AI- and network-specialized education and training solutions.

### 6.3. High Initial Costs

Deploying AI for networking demands massive upfront investment [39]. Costs are incurred on the purchase of high-performance computing hardware, acquisition of AI software licenses, and employing qualified individuals. Small businesses will most likely consider these expenditures as being high [40]. While AI is claimed to save costs in the long run, the upfront cost acts as a deterrent to most firms.

### 6.4. Model Transparency and Interpretability

The majority of the AI techniques, particularly those based on deep learning, are "black boxes" in that what decision was made and how they made it is not transparent. In networking, where timing is of the essence and decisions have implications on important services, transparency is paramount [41]. Understanding the reason behind the decision by an AI system for a particular routing or security decision is needed for trust, compliance, and debugging. There has been growing work in explainable AI (XAI) to meet this demand [42].

### 6.5. Integration Complexity

Integration of AI systems with current networking hardware is also a significant challenge. Incompatibility, absence of standards, and resistance to change will impede rollout [43]. Seamless integration will require a stepped transition approach, potentially on hybrid systems that combine AI-empowered modules with current network management hardware.

## VII. FUTURE DIRECTIONS FOR AI NETWORKING DEVELOPMENT

As tomorrow's networks will impose more challenges with expansion in cloud, IoT, 5G, etc., the application of Artificial Intelligence (AI) in networking will itself evolve with time [44]. The future will be filled with innovations in terms of making the network smart, autonomous, and resilient. Some of the most significant future trends for AI-networking are provided below:

### 7.1. Autonomous Networks and Zero-Touch Automation

The long-term vision for AI networking is the formation of independently functioning networks—networks that can be managed, configured, optimized, and healed without any human intervention [45]. This vision, otherwise referred to as "zero-touch networking," will dominate the coming years. Using AI algorithms on intent-based networking (IBN), networks will transform high-order user intention into automated network action [46]. This transformation will reduce operational costs, eliminate configuration defects, and improve responsiveness to perpetually changing network conditions.

### 7.2. AI Edge Computing Integration

The edge computing age demands intelligent processing near or even at the edge of data source generation [47]. Edge AI will be the hub for managing local network behaviour such as traffic filtering, security, and QoS management without crossing centralized data centers. It supports low-latency real-time decision-making, which is necessary for mission-critical applications like autonomous vehicles and industrial control [48]. The future will see AI models designed to optimize edge devices and decentralized network topologies.

### 7.3. Next-Generation AI for Cybersecurity

As cyber threats continue to evolve, AI will play a central role in network security via predictive threat modelling, pre-emptive countermeasures, and real-time restoration [48]. Next-generation AI systems will not only detect and respond to

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 6, June 2025

DOI: 10.17148/IARJSET.2025.12649

known threats but also forecast novel attack channels based on learning global threat intelligence. Federated learning and homomorphic encryption will also support secure model training without sensitive information leakage.

### 7.4. Explainable and Ethical AI Systems

Among the most significant limitations of current AI systems is that they are not transparent. As AI-based decisions come to the forefront in critical network functions, the need for explainable AI (XAI) will grow [49]. XAI systems will provide explanations on why and how some network actions are being done, enabling trust and regulatory acceptance. Second, ethical frameworks will need to be embedded in AI in a bid to promote fairness, accountability, and protection of privacy.

### 7.5. Interoperability and Standardization

Open standards and industry platforms will also determine the future of AI in the network environment. Industry players and standards bodies (e.g., IEEE and IETF) will need to work together and establish standard data formats, integration styles, and protocols [50]. This will enable interoperability and deployment of AI in multi-vendor networks.

To get to the point, AI networked networking's future is greater intelligence, greater autonomy, and moral responsibility [51]. These developments will not only remake network control but redefine what the world's digital infrastructure can offer.

## VIII. CONCLUSION

Artificial Intelligence (AI) emerged as a paradigm shift in the evolution of communication infrastructure. As networks are becoming more complicated, dynamic, and an inherent part of the way society functions today, traditional management solutions cannot keep pace with the speed, scalability, and efficiency required to meet the demand. AI is an entity that brought about a breakthrough with intelligent automation, real-time decision-making, and maximization of predictability in all aspects of network operation.

We discussed in this article how the aforementioned AI technologies, such as machine learning, deep learning, and reinforcement learning, are being used to solve basic network issues. From fault detection and traffic control to security and QoS enhancement, AI has been able to demonstrate its potential to enhance network reliability and performance. Google, Cisco, and Facebook are some of the organizations that have already applied AI-based technologies to production, which says a lot about the use of such technologies in the real world.

AI use in networking has a number of advantages. It maximizes spend by automating, maximizes network efficiency with optimal usage of resources, maximizes security with smart discovery of attacks, and enables scalability through dynamic, responsive control. All these advantages are not just beneficial to large-scale carriers but also to corporate, governmental agencies, even small and medium enterprises who wish to upgrade their digital infrastructure.

But reaching there is not simple. Enabling previous impediments to implementation such as cost, model interpretability, data privacy, and legacy system integration need to be addressed before AI can fulfill promise. And also, lacking sufficient trained professionals in AI, along with network effects, are primary to-be inhibitors for deployment across the world.

In the years to come, the future of AI in networking is vast and hopeful. AI edge, self-managing networks, and transparent AI systems will keep pushing the limits of what can be achieved with intelligent networks. Joint initiatives from the industry towards standardization and ethics in AI development will render such types of systems credible, transparent, and lucrative for all stakeholders.

In brief, AI is not merely a network upgrade anymore but also the foundation of future network architecture. Its ability to learn, develop, and adapt in real time makes it a precious resource to build bulletproof, efficient, and future-proofed networks. Those who are set to gain from this transition will be well placed to meet the challenge of an increasingly digitally networked world.

## REFERENCES

[1]. Knapp, E. D. (2024). *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Elsevier.

[2]. Mistry, H. K., Mavani, C., Goswami, A., & Patel, R. (2024). Artificial intelligence for networking. *Educational Administration: Theory and Practice*, *30*(7), 813-821.

[3]. Mohammed, A. K., & Ansari, M. A. (2024). The Impact and Limitations of AI in Power BI: A Review. International Journal of Multidisciplinary Research and Publications (IJMRAP),. Pp. 23-27, 2024., 7(7), 24–27.

 

DOI: 10.17148/IARJSET.2025.12649

[4]. Chittoju, S. R., & Ansari, S. F. (2024). Blockchain's Evolution in Financial Services: Enhancing Security, Transparency, and Operational Efficiency. International Journal of Advanced Research in Computer and Communication Engineering, 13(12), 1–5. https://doi.org/10.17148/IJARCCE.2024.131201

[5]. Thakkar, A., & Lohiya, R. (2022). A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions. *Artificial Intelligence Review*, *55*(1), 453-563.

[6]. Siriwardhana, Y., Porambage, P., Liyanage, M., & Ylianttila, M. (2021). A survey on mobile augmented reality with 5G mobile edge computing: Architectures, applications, and technical aspects. *IEEE Communications Surveys & Tutorials*, *23*(2), 1160-1192.

[7]. Khadri, W., Reddy, J. K., Mohammed, A., & Kiruthiga, T. (2024, July). The Smart Banking Automation for High Rated Financial Transactions using Deep Learning. In 2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC) (pp. 686-692). IEEE.

[8]. Janamolla, K., Balammagary, S., & Mohammed, A. Blockchain Enabled Cybersecurity to Protect LLM Models in FinTech.

[9]. Sarker, I. H. (2021). Deep learning: a comprehensive overview on techniques, taxonomy, applications and research directions. *SN computer science*, *2*(6), 1-20.

[10]. Sharma, A., Gupta, B. B., Singh, A. K., & Saraswat, V. K. (2023). Advanced persistent threats (apt): evolution, anatomy, attribution and countermeasures. *Journal of Ambient Intelligence and Humanized Computing*, *14*(7), 9355-9381.

[11]. Shakya, A. K., Pillai, G., & Chakrabarty, S. (2023). Reinforcement learning algorithms: A brief survey. *Expert Systems with Applications*, *231*, 120495.

[12]. Fanni, S. C., Febi, M., Aghakhanyan, G., & Neri, E. (2023). Natural language processing. In *Introduction to artificial intelligence* (pp. 87-99). Cham: Springer International Publishing.

[13]. Mohammed, A., Mohammed, N. U., Gunda, S. K. R., & Mohammed, Z. Fundamental Principles of Network Security

[14]. Nigam, N., Singh, D. P., & Choudhary, J. (2023). A review of different components of the intelligent traffic management system (ITMS). *Symmetry*, *15*(3), 583.

[15]. Khadri Syed, W., & Janamolla, K. R. (2023). Fight against financial crimes – early detection and prevention of financial frauds in the financial sector with application of enhanced AI. IJARCCE, 13(1), 59–64. https://doi.org/10.17148/ijarcce.2024.13107

[16]. Gadde, H. (2024). AI-Powered Fault Detection and Recovery in High-Availability Databases. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, *15*(1), 500-529.

[17]. Mazhar, T., Malik, M. A., Mohsan, S. A. H., Li, Y., Haq, I., Ghorashi, S., ... & Mostafa, S. M. (2023). Quality of service (QoS) performance analysis in a traffic engineering model for next-generation wireless sensor networks. *Symmetry*, *15*(2), 513.

[18]. Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. *SN computer science*, *2*(3), 160.

[19]. McGuirk, M. (2023). Performing web analytics with Google Analytics 4: a platform review. *Journal of Marketing Analytics*, *11*(4), 854-868.

[20]. Alatalo, M. (2022). Cisco Secure Network Analytics (Stealthwatch).

[21]. Syed, W. K., Mohammed, A., Reddy, J. K., & Dhanasekaran, S. (2024, July). Biometric Authentication Systems in Banking: A Technical Evaluation of Security Measures. In 2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC) (pp. 1331-1336). IEEE.

[22]. Fronteddu, R. (2022). Computer Networks In Tactical And Disaster Recovery Environments.

[23]. Balammagary, S., Mohammed, N., Mohammed, S., & Begum, A. (2025). AI-Driven Behavioural Insights for Ozempic Drug Users. Journal of Cognitive Computing and Cybernetic Innovations, 1(1), 10-13.

[24]. Mohammed, A., Sultana, G., Aasimuddin, F. M., & Mohammed, S. (2025). Leveraging Natural Language Processing for Trade Exception Classification and Resolution in Capital Markets: A Comprehensive Study. Journal of Cognitive Computing and Cybernetic Innovations, 1(1), 14-18.

[25]. Szalavetz, A. (2023). Digital technologies shaping the nature and routine intensity of shopfloor work. *Competition & Change*, *27*(2), 277-301.

[26]. Tan, M., & Le, Q. (2021, July). Efficientnetv2: Smaller models and faster training. In *International conference on machine learning* (pp. 10096-10106). PMLR.

[27]. Mohammed, S., DDS, Dr. S. T. A., Mohammed, N., & Sultana, W. (2024). A review of AI-powered diagnosis of rare diseases. International Journal of Current Science Research and Review, 07(09). https://doi.org/10.47191/ijcsrr/v7-i9-01

[28]. Jimmy, F. N. U. (2023). Cloud security posture management: tools and techniques. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(3).

 

DOI: 10.17148/IARJSET.2025.12649

[29]. De Neira, A. B., Kantarci, B., & Nogueira, M. (2023). Distributed denial of service attack prediction: Challenges, open issues and opportunities. *Computer Networks*, *222*, 109553.

[30]. Shi, C., Peng, J., Zhu, S., & Ren, X. (2023, December). From passive defense to proactive defence: Strategies and technologies. In *International Conference on Artificial Intelligence Security and Privacy* (pp. 190-205). Singapore: Springer Nature Singapore.

[31]. Solano, N. E. C., Llinás, G. A. G., & Montoya-Torres, J. R. (2022). Operational model for minimizing costs in agricultural production systems. *Computers and Electronics in Agriculture*, *197*, 106932.

[32]. Begum, A., Mohammed, N., & Panda, B. B. (2024). Leveraging AI in health informatics for early diagnosis and disease monitoring. IARJSET, 11(12), 71–79. https://doi.org/10.17148/iarjset.2024.111205

[33]. Mohammed, Z., Mohammed, N. U. M., Mohammed, A., Gunda, S. K. R., & Ansari, M. A. A. (2025). AI-Powered Energy Efficient and Sustainable Cloud Networking. Journal of Cognitive Computing and Cybernetic Innovations, 1(1), 31-36.

[34]. Xu, B., Li, Y., & Wei, Z. (2024). Familiarize Students with Direct MS Analysis Methods: Localization of Components in Citrus Peel by Induced Electrospray Ionization. *Journal of Chemical Education*, *101*(6), 2429-2435.

[35]. Zhang, Y., Zhang, C., & Xu, Y. (2021). Effect of data privacy and security investment on the value of big data firms. *Decision Support Systems*, *146*, 113543.

[36]. Liu, H., Li, K., Chen, Y., & Luo, X. R. (2023). Is personally identifiable information really more valuable? Evidence from consumers' willingness-to-accept valuation of their privacy information. *Decision Support Systems*, *173*, 114010.

[37]. S. Mohammed, Z. A. Mohammed, A. A. Doctor, R. Gupta, K. Gupta and S. D. Sekaran, "Intelligent Edge Computing for Real-Time Tumor Detection Using Machine Learning," 2024 2nd International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), Faridabad, India, 2024, pp. 462-467, doi: 10.1109/ICAICCIT64383.2024.10912155.

[38]. Arora, S., & Tewari, A. (2022). AI-Driven Resilience: Enhancing Critical Infrastructure with Edge Computing. *Int. J. Curr. Eng. Technol*, *12*(2), 151-157.

[39]. Zhang, T., Qiu, H., Mellia, M., Li, Y., Li, H., & Xu, K. (2022). Interpreting AI for networking: Where we are and where we are going. *IEEE Communications Magazine*, *60*(2), 25-31.

[40]. Contractor, D., McDuff, D., Haines, J. K., Lee, J., Hines, C., Hecht, B., ... & Li, H. (2022, June). Behavioral use licensing for responsible AI. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (pp. 778-788).

[41]. Petch, J., Di, S., & Nelson, W. (2022). Opening the black box: the promise and limitations of explainable machine learning in cardiology. *Canadian Journal of Cardiology*, *38*(2), 204-213.

[42]. Gunning, D., Vorm, E., Wang, Y., & Turek, M. (2021). DARPA's explainable AI (XAI) program: A retrospective. *Authorea Preprints*.

[43]. Wermke, W., & Prøitz, T. S. (2021). 13 Integration, fragmentation, and complexity. *Schoolteachers and the Nordic model*, 216.

[44]. Gill, S. S., Xu, M., Ottaviani, C., Patros, P., Bahsoon, R., Shaghaghi, A., ... & Uhlig, S. (2022). AI for next generation computing: Emerging trends and future directions. *Internet of Things*, *19*, 100514.

[45]. El Rajab, M., Yang, L., & Shami, A. (2024). Zero-touch networks: Towards next-generation network automation. *Computer Networks*, *243*, 110294.

[46]. Mohammed, Shanavaz. "The Impact of AI on Clinical Trial anagement."(2024b).

[47]. Hossain, M. E., Tarafder, M. T. R., Ahmed, N., Al Noman, A., Sarkar, M. I., & Hossain, Z. (2023). Integrating AI with Edge Computing and Cloud Services for Real-Time Data Processing and Decision Making. *International Journal of Multidisciplinary Sciences and Arts*, *2*(4), 252-261.

[48]. Bowman, B., & Huang, H. H. (2021). Towards next-generation cybersecurity with graph AI. *ACM SIGOPS Operating Systems Review*, *55*(1), 61-67.

[49]. Gunning, D., Vorm, E., Wang, Y., & Turek, M. (2021). DARPA's explainable AI (XAI) program: A retrospective. *Authorea Preprints*.

[50]. Khare, P., Karan, M., McQuistin, S., Perkins, C., Tyson, G., Purver, M., ... & Castro, I. (2022, May). The web we weave: Untangling the social graph of the IETF. In *Proceedings of the International AAAI Conference on Web and Social Media* (Vol. 16, pp. 500-511).

[51]. Song, L., Hu, X., Zhang, G., Spachos, P., Plataniotis, K. N., & Wu, H. (2022). Networking systems of AI: On the convergence of computing and communications. *IEEE Internet of Things Journal*, *9*(20), 20352-20381.

 