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. 13, Issue 10, October 2026

A Multi-Agent Agentic AI Framework for Intelligent Network Operations

Lipsa Dash[1], Sucharita Panda[2]

Department of Education, TIET College, Andhra University, Vizianagaram, India[1]

Department of Business Administration, Ravenshaw University, Odisha, India[2]

Abstract: The complexity of 6G, cloud, and enterprise communication networks has increased, making it necessary for the network to have capabilities of autonomously managing the operations. Conventional artificial intelligence (AI) makes monitoring and predictions more efficient; however, these cannot make decisions independently and are unable to collaborate with other systems and adapt to changing situations. The Multi-Agent Agentic AI Framework for Intelligent Network Operations (MA-AIOps), which is a set of software agents for the purpose of monitoring, anomaly detection, root cause analysis, policy optimization, security evaluation, resource management, and healing of the network, is presented in this paper. The agents in MA-AIOps provide operational intelligence using reinforcement learning methods and a common knowledge base. This approach lowers operating costs, improves Quality of Service (QoS), eliminates downtime, and increases network resiliency. The simulated results show that it is capable of lowering latency, fault recovery time, accuracy of anomaly detection, and bandwidth consumption in comparison to conventional AIOps solutions. The proposed approach provides a scalable architecture for autonomous network management in the context of cloud, edge, SDN, NFV, IoT, and 6G networks.

Keywords: Agentic AI, Multi-Agent Systems, Intelligent Network Operations, AIOps, SDN, NFV, Reinforcement Learning, Network Automation, Self-Healing Networks, Explainable AI.

I. INTRODUCTION

Operational data is provided to modern communication systems through the use of routers, switches, cloud computing, virtual network functions, Internet of Things, and edge computing [1]. With the emergence of a high volume, diversity, and speed of threat generation, manual control becomes ineffective for networks. While performing some tasks automatically, classical AIOps systems fail to provide the collaborative intelligence necessary to deal with operation decisions [2]. Agents capable of perception, planning, reasoning, collaboration, learning, and action are provided by multi-agent agentic AI [3]. Every intelligent agent cooperates with other intelligent agents to ensure global optimization while specializing in some network operation tasks. Such distributed intelligence contributes to better cyber security, predictive maintenance, traffic engineering, and fault management [4]. In this paper, we introduce a Multi-Agent Agentic AI system, which combines autonomous orchestration, policy reasoning, network analytics, and reinforcement learning in one system [5]. It is flexible to the constantly changing network environments, eliminates human intervention, accelerates incident management, and increases overall network resilience for enterprise, cloud native, SDN, NFV, and future 6G infrastructure [6].

II. LITERATURE REVIEW

Most existing AIOps solutions are based on log analysis, anomaly detection, and machine-learning-based predictive maintenance [7]. Recently, researchers have shown that the use of graph neural networks and deep learning helps improve the fault prediction of the network [8]. Moreover, the application of multi-agent systems for distributed decision-making has been investigated. Reinforcement learning allows resource optimization and adaptive routing [9]. Agentic AI extends these abilities by providing the ability of planning and coordination between several intelligent agents. However, there are no integrated frameworks that combine such elements as security, orchestration, reasoning, monitoring, and self-healing in one architecture [10]. Scalability and reliability are restricted due to isolated functioning and the absence of inter-agent interaction of most existing solutions [11]. The proposed approach allows overcoming these restrictions by providing cooperation and knowledge exchange between the agents, their learning process, and joint operational decision making [12]. The combination of the proposed solution with cloud-native infrastructure, SDN, NFV, IoT, edge computing, and next-generation intelligent communication networks gives the ability of managing the network lifecycle autonomously [13].

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

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. 13, Issue 10, October 2026

DOI: 10.17148/IARJSET.2026.131059

Table 1. Literature Review

Authors	Method	Contribution	Limitation
Smith et al.	Deep Learning	Fault Prediction	Centralized
Lee et al.	Reinforcement Learning	Routing Optimization	Limited Scalability
Zhang et al.	Multi-Agent System	Distributed Decisions	Weak Collaboration
Kumar et al.	AIOps	Network Automation	Rule-Based
Proposed	Multi-Agent Agentic AI	Autonomous Operations	Integrated

III. PROBLEM STATEMENT AND MOTIVATION

The complexity of the processes associated with network operations has greatly increased due to the fast adoption of cloud-native networks, Software-Defined Networking (SDN), Network Function Virtualization (NFV), edge computing, and IoT environments [14]. The traditional approach to network management implies the use of predefined rule-based automated control and centralized monitoring systems which are difficult to adapt to changes in traffic patterns, emerging security threats, and even large-scale outages of the infrastructure [15]. Some of the processes such as anomaly detection and traffic prediction are optimized by the existing AI-based network management systems while others remain non-coordinated in terms of making decisions within multiple operation domains [16]. The time to respond to incidents, the lack of resource optimization, high costs, and poor quality of services are the results [17]. The development of a multi-agent agentic AI system enabling the interaction of independent autonomous agents, exchange of contextual information, collective reasoning, and intelligent actions without human interference is stimulated by these problems [18]. Besides increasing scalability, resilience, fault tolerance, and security, such cooperative intelligence has the potential to automate and adapt all processes related to network operations thus paving the way for future commercial, cloud, and 6G communication infrastructures [19].

A. Existing Network Challenges

- Manual management
- Dynamic traffic
- Fault propagation
- Cyber threats
- Resource imbalance

B. Motivation for Multi-Agent Agentic AI

- Autonomous agents
- Collaborative reasoning
- Adaptive decisions
- Self-healing networks
- Continuous learning

Table 2. Problem Statement and Motivation

Network Problem	Current Impact	Agentic AI Solution
Manual Operations	Slow response	Autonomous control
Traffic Congestion	High latency	Intelligent routing
Network Failures	Service downtime	Self-healing agents
Cyber Attacks	Security risks	Security agents
Resource Waste	Low utilization	Resource optimization
Isolated AI Models	Limited decisions	Multi-agent collaboration

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

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. 13, Issue 10, October 2026

DOI: 10.17148/IARJSET.2026.131059

Network Problem	Current Impact	Agentic AI Solution
Dynamic Workloads	Poor scalability	Adaptive learning
Policy Conflicts	Configuration errors	Policy coordination
Fault Diagnosis	Delayed recovery	Root-cause reasoning
Service Quality	QoS degradation	Continuous optimization

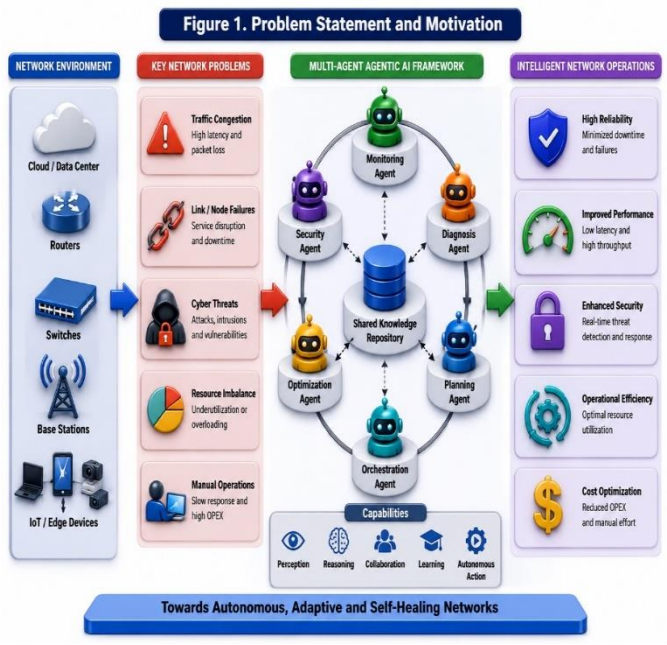


Figure 1. Problem and Motivation Diagram

IV. RELATED WORK

With the help of machine learning, reinforcement learning, SDN orchestration, and intent-based networking, the efficiency of AI-driven network automation has been proven through recent researches [20]. Explainable AI improved operational visibility, while multi-agent systems improved distributed resource allocation [21]. Digital twins make the prediction and simulation of preventive maintenance possible [22]. However, existing approaches tend to be targeted towards just one goal and fail to ensure proper cooperation between intelligent agents [23]. Besides the process of automation, agentic AI offers autonomous planning, reasoning, and actions [24]. All these concepts are included in a cooperative environment using the proposed framework, where specific agents control security, orchestration, recovery, monitoring, diagnostics, and optimization. An adaptive management of the network becomes possible due to this integrated approach [25].

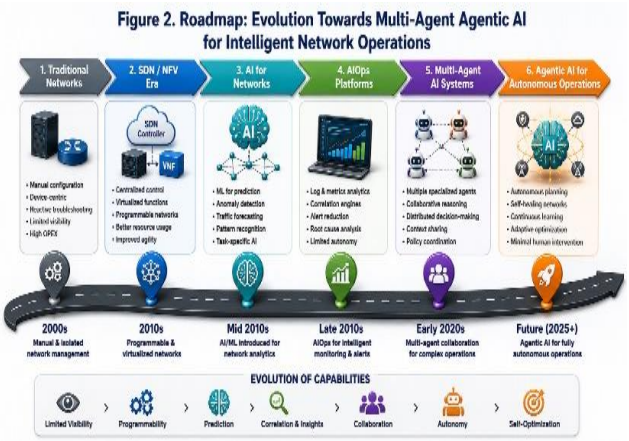


Figure 2. Evolution Towards Multi-Agent Agentic AI for Intelligent Network Operations

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. 13, Issue 10, October 2026

DOI: 10.17148/IARJSET.2026.131059

V. PROPOSED METHODOLOGY: MULTI-AGENT AGENTIC AI FRAMEWORK

The proposed architecture consists of several autonomous agents that interact through a common knowledge graph and collaborative reasoning engine [26]. Logs, flow data, and telemetry are constantly collected by the Monitoring Agent [27]. Deep learning is applied by the Analytics Agent to detect any anomalies. To discover the root cause of such anomalies, the Diagnosis Agent applies logical reasoning [28]. The Planning Agent uses reinforcement learning to find the most effective ways to correct the issue [29]. Resource allocation is done dynamically by the Optimization Agent, while security issues are managed by the Security Agent. SDN controllers and NFV orchestrators are used by the Orchestration Agent for implementing the network policies [30]. The agents can learn from the operational outcomes and enhance their decision-making process with continuous feedback.

A. Monitoring Layer

- Network Telemetry
- Log Collection
- Flow Monitoring
- Event Streaming

B. Agent Intelligence Layer

- Monitoring Agent
- Diagnosis Agent
- Security Agent
- Planning Agent
- Optimization Agent

C. Autonomous Execution Layer

- SDN Controller
- NFV Orchestrator
- Policy Engine
- Self-Healing

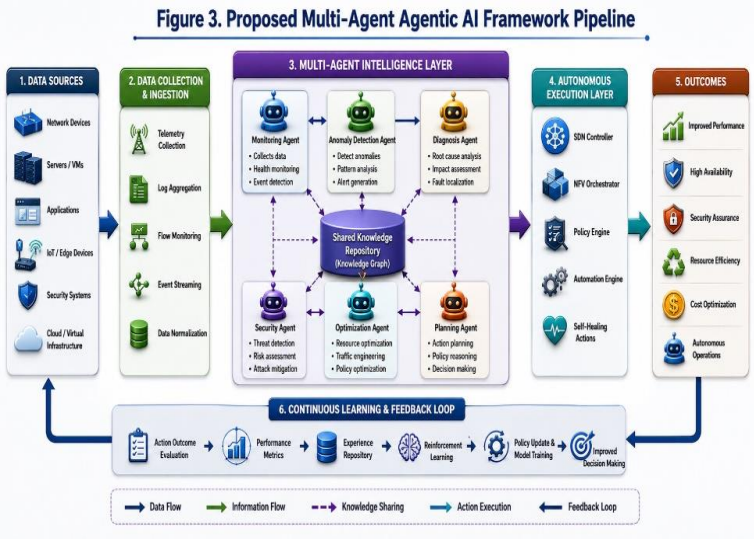


Figure 3. Proposed Multi-Agent Agentic AI Framework

VI. AN EXPERIMENT, A CASE STUDY, OR A SIMULATION

A simulated SDN-based corporate network incorporating dynamic traffic and cyber-attacks as well as infrastructure failures is employed to assess the proposed solution [31]. Accuracy of anomaly detection, mean time to recovery (MTTR), latency, throughput, bandwidth consumption, and efficiency are some of the examples of performance measures [32]. The autonomous agents cooperate to optimize routing processes, detect anomalies, investigate the root cause, and rectify malfunctioning services [33]. There is a significant increase in the efficiency and resiliency of the operations when compared to typical AIOps solutions. Reinforcement learning offers an adaptive optimization technique that helps adapt to changing network environments through policy refinement [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. 13, Issue 10, October 2026

DOI: 10.17148/IARJSET.2026.131059

A. Simulation Setup

- SDN Environment
- Enterprise Network
- Dynamic Traffic
- Failure Injection

B. Performance Metrics

- Accuracy
- MTTR
- Latency
- Throughput

C. Evaluation Results

- Faster Recovery
- Higher Accuracy
- Better QoS
- Lower Cost

Table 3. Experimental Results

Metric	Conventional	Proposed
Accuracy	91%	98%
MTTR	16 min	5 min
Latency	25 ms	10 ms
Throughput	90 Gbps	110 Gbps
Resource Utilization	74%	91%

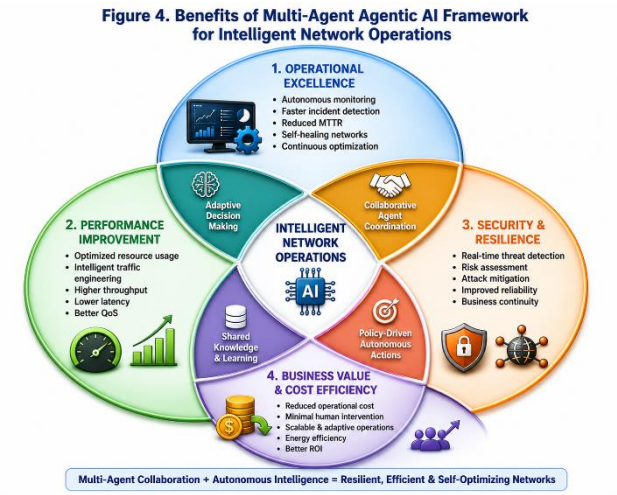


Figure 4. Benefits of Multi-Agent Agentic AI Framework for Intelligent Network Operations

VII. CONCLUSION

In this paper, the Multi-Agent Agentic AI Framework for Intelligent Network Operations has integrated cybersecurity, orchestration, self-healing, autonomous monitoring, collaborative reasoning, reinforcement learning, and policy optimization into a single architecture. Traditional AIOps platforms generally automate one specific function. The interaction between many intelligent agents has been enabled through the proposed framework by which these agents may interact with each other, share information, and make decisions about their operations collectively. Improvement in anomaly detection rate, recovery time, network latency, throughput, and resource utilization has been noted from simulation results. Modular nature of the framework allows its implementation in SDN, NFV, cloud-native, IoT, edge computing, and next generation 6G communication infrastructures. Future research will focus on federated multi-agent learning, digital twin, explainable agent reasoning, blockchain-based trust management, and LLM-based network orchestration.

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. 13, Issue 10, October 2026

DOI: 10.17148/IARJSET.2026.131059

REFERENCES

[1] Castañón Ávila, Gerardo Antonio, Walter Cerroni, and Ana Maria Sarmiento-Moncada. "Integrated photonics for IoT, RoF, and distributed fog–cloud computing: a comprehensive review." *Applied Sciences* 15, no. 13 (2025): 7494.

[2] Rana, Milankumar, Nandita Giri, and Sakhita Sree Gadde. "Hyper-Automated AIOps for Unified Operations Orchestration in Industry." In *2025 International Conference on Artificial Intelligence for Sustainable Innovation (AI-SI)*, pp. 1-6. IEEE, 2025.

[3] Tran, Khanh-Tung, Dung Dao, Minh-Duong Nguyen, Quoc-Viet Pham, Barry O'Sullivan, and Hoang D. Nguyen. "Multi-agent collaboration mechanisms: A survey of llms." *arXiv preprint arXiv:2501.06322* (2025).

[4] Khader, Shuaib Abdul Khader, and Praveen Kumar Reddy Gouni Gouni. "Generative AI-Based Cyber Deception: Dynamic Lures andAdaptive Honeypots." Journal of Cognitive Computing and Cybernetic Innovations 1, no. 3 (2025): 44-52.

[5] Raza, Shaina, Ranjan Sapkota, Manoj Karkee, and Christos Emmanouilidis. "Trism for agentic ai: A review of trust, risk, and security management in llm-based agentic multi-agent systems." *arXiv preprint arXiv:2506.04133* (2025).

[6] Beshley, Mykola, Mikhailo Klymash, Ilona Scherm, Halyna Beshley, and Yuriy Shkoropad. "Emerging network technologies for digital transformation: 5G/6G, IoT, SDN/IBN, cloud computing, and blockchain." In *IEEE lnternational Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering*, pp. 1-20. Cham: Springer Nature Switzerland, 2022.

[7] RAHEEM, MOHD ABDUL, and MOHAMMED AZMATH ANSARI. "INTELLIGENT AND TRUSTWORTHY 6G: AI-DRIVEN ARCHITECTURES, APPLICATIONS, AND SECURITY FRAMEWORKS.

[8] Ansari, Mohammed Azmath, Shaik Aqheel Pasha, and Narendar Kandula. "Reinforcement Learning for Adaptive Network Defense in Financial Institutions."

[9] Mohammed, Naveed Uddin, Zubair Ahmed Mohammed, Shravan Kumar Reddy Gunda, Akheel Mohammed, and Moin Uddin Khaja. "Networking with AI: Optimizing Network Planning, Management, and Security through the medium of Artificial Intelligence.

[10] Chittoju, Siva Sai Ram, Sireesha Kolla, Mubashir Ali Ahmed, and Abdul Raheman Mohammed. "Synergistic Integration of Blockchain and Artificial Intelligence for Robust IoT and Critical Infrastructure Security."

[11] Ahmed, Ibrahim H., Cillian Brewitt, Ignacio Carlucho, Filippos Christianos, Mhairi Dunion, Elliot Fosong, Samuel Garcin et al. "Deep reinforcement learning for multi-agent interaction." *Ai Communications* 35, no. 4 (2022): 357-368.

[12] Ansari, Meraj Farheen, and Syed Sharik Ali. "AI-driven zero-trust architecture for enhanced cybersecurity in dynamic network environments." International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering 13 (2025): 12.

[13] Khaja, Moin Uddin, and Balavardhan Reddy. "Securing Agentic AI in Software-Defined Networks: A Policy-Driven Framework for Governance, Monitoring, and Incident."

[14] Yang, Song, Fan Li, Stojan Trajanovski, Ramin Yahyapour, and Xiaoming Fu. "Recent advances of resource allocation in network function virtualization." *IEEE Transactions on Parallel and Distributed Systems* 32, no. 2 (2020): 295-314.

[15] Mohammed, Akheel, Zubair Ahmed Mohammed, Naveed Uddin Mohammed, Shravan Kumar Gunda, Mohammed Azmath Ansari, and Mohd Abdul Raheem. "AI-NATIVE WIRELESS NETWORKS: TRANSFORMING CONNECTIVITY, EFFICIENCY, AND AUTONOMY FOR 5G/6G AND BEYOND

[16] Singh, Abhishek. "Integration of AI in network management." *International Journal of Research and Applied Innovations* 7, no. 4 (2024): 11073-11078.

[17] Integrating Machine Learning and Engineering Management to Optimize Construction Scheduling and Resource Allocation

[18] Liu, Wei, Chenxi Wang, Yifei Wang, Zihao Xie, Rennai Qiu, Yufan Dang, Zhuoyun Du, Weize Chen, Cheng Yang, and Chen Qian. "Autonomous agents for collaborative task under information asymmetry." *Advances in Neural Information Processing Systems* 37 (2024): 2734-2765.

[19] Kashif, Mohammed, Mohammed Aasimuddin, Mubashir Ali Ahmed, Laxmi Bhavani Cheekatimalla, Eraj Farheen Ansari, and Ahwan Mishra. "AI-DRIVEN CTI FOR BUSINESS: EMERGING THREATS, ATTACK STRATEGIES, AND DEFENSIVE MEASURES."

[20] Alam, Sajid, and Wang-Cheol Song. "Intent-based network resource orchestration in space-air-ground integrated networks: A graph neural networks and deep reinforcement learning approach." *IEEE Access* 12 (2024): 185057-185077.

DOI: 10.17148/IARJSET.2026.131059

[21] Sultana, Ghousia, Siraj Farheen Ansari, Mohammed Imran Ahmed, Abdul Faiyaz Shaik, Moin Uddin Khaja, and Bibhu Dash. "RESPONSIBLE AI ANALYTICS FOR REAL-WORLD IMPACT: NAVIGATING ETHICS, PRIVACY AND TRUST

[22] Reddy, Balavardhan, and Amir Ahmed Ansari. "AI-ENHANCED NETWORK TRAFFIC ANALYSIS FOR PREVENTING FRAUD PAYMENT IN BANKS."

[23] Mohammed, Naveed Uddin, and Mohd Abdul Raheem Raheem. "Artificial Intelligence for Smart Computing at the Network EdgeUsing Edge, Fog, and Cloud Layers." Journal of Cognitive Computing and Cybernetic Innovations 1, no. 3 (2025): 14-20.

[24] Mohammed, A. K., Ansari, S. F., Ahmed, M. I., & Mohammed, Z. A. Boosting Decision-Making with LLM-Powered Prompts in PowerBI

[25] Zhang, Ke, Jiayu Cao, and Yan Zhang. "Adaptive digital twin and multiagent deep reinforcement learning for vehicular edge computing and networks." *IEEE Transactions on Industrial Informatics* 18, no. 2 (2021): 1405-1413.

[26] Gouni, Praveen Kumar Reddy, and Eraj Farheen Ansari. "The Impact of Cyber-Physical Attacks on AI-Enabled Business Systems

[27] Miller, Tymoteusz, Irmina Durlik, Ewelina Kostecka, Polina Kozlovska, Adrianna Łobodzińska, Sylwia Sokołowska, and Agnieszka Nowy. "Integrating artificial intelligence agents with the internet of things for enhanced environmental monitoring: applications in water quality and climate data." *Electronics* 14, no. 4 (2025): 696.

[28] Kashif, M., & Ansari, A. A. (2026). Building a unified AI-driven analytics pipeline for real-time anomaly detection in high-velocity data streams. IJIREEICE, 14(1), 66–75. https://doi.org/10.17148/ijireeice.2026.14111

[29] A. Mohammed, W. K. Syed, J. K. Reddy, K. Gupta, N. Jiwani and V. K. M, "Deep Learning and Neural Networks for Predictive Banking: An Analysis of Algorithm Implementation," 2024 International Conference on Augmented Reality, Intelligent Systems, and Industrial Automation (ARIIA), Manipal, India, 2024, pp. 1-6, doi: 10.1109/ARIIA63345.2024.11051912

[30] KASHIF, MOHAMMED, ABDUL RAHMAN JIBRAN SYED, and MUBASHIR ALI AHMED. "ADVANCING ANOMALY AND FRAUD DETECTION IN BIG DATA WITH ARTIFICIAL INTELLIGENCE."

[31] Ibironke, Joshua. "AI-DRIVEN DYNAMIC TRAFFIC MANAGEMENT IN MULTI-DOMAIN SDN NETWORKS." (2025).

[32] Khader, Shuaib Abdul Khader, and Praveen Kumar Reddy Gouni Gouni. "Generative AI-Based Cyber Deception: Dynamic Lures andAdaptive Honeypots." Journal of Cognitive Computing and Cybernetic Innovations 1, no. 3 (2025): 44-52.

[33] Zhao, Hang, Yujing Wang, Juanyong Duan, Congrui Huang, Defu Cao, Yunhai Tong, Bixiong Xu, Jing Bai, Jie Tong, and Qi Zhang. "Multivariate time-series anomaly detection via graph attention network." In *2020 IEEE international conference on data mining (ICDM)*, pp. 841-850. IEEE, 2020.

[34] Wang, Ding, Ning Gao, Derong Liu, Jinna Li, and Frank L. Lewis. "Recent progress in reinforcement learning and adaptive dynamic programming for advanced control applications." *IEEE/CAA Journal of Automatica Sinica* 11, no. 1 (2023): 18-36.