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

Multi-Agent Agentic AI for Real-Time Clinical Decision Support and Healthcare Security

Rudra Narayan Dash

Department of Computer Science and Engineering, Roland Institute of Technology, Berhampur,India

Abstract: Given the fast expansion of the digital healthcare frameworks, the need for cognitive clinical decision support is evident; however, vital medical frameworks are prone to highly sophisticated cyberattacks. By enabling collaborative clinical analysis, security monitoring, medical knowledge acquisition, risk assessment, and decision-making validation when several specialized AI agents cooperate in real-time, Multi-Agent Agentic Artificial Intelligence (MAAI) framework develops an independent, collaborative, and adaptive framework. In order to increase the precision of diagnosis, reaction rate, privacy assurance, and resilience of the operations, we propose Multi-Agent Agentic AI framework in this paper, which combines clinical intelligence with healthcare cybersecurity. Respecting the standards of healthcare, the proposed architecture enables secure data transmission from wearable devices, cloud-edge infrastructures, laboratory frameworks, and EHRs. Unlike existing AI-driven healthcare systems, experimental evaluation indicates improvements in terms of resource management, detection efficiency, prediction performance, and decision delay. The proposed architecture provides the basis for future intelligent clinical environments by offering reliable, interpretable, and secure healthcare services to hospitals, telemedicine frameworks, and smart healthcare ecosystems.

Keywords: Multi-Agent AI, Agentic AI, Clinical Decision Support, Healthcare Security, Electronic Health Records, Cybersecurity, Explainable AI, Medical AI, Edge Computing, Healthcare Analytics

I. INTRODUCTION

Healthcare institutions have started relying on technologies like IT, cloud computing, electronic health records, and connected devices for provision of efficient services to patients [1]. Heterogeneous medical data and new cybersecurity issues are normally an issue in conventional clinical decision support systems [2]. For providing diagnosis, treatments, patient monitoring, threat identification, and policy implementation, Multi-Agent Agentic AI utilizes self-sufficient agents [3]. Unlike conventional AI systems, several intelligent agents constantly exchange information, coordinate decisions, and adapt to new clinical situations with minimal help from human beings [4]. Ransomware attacks, insider threats, and illegal access to confidential patient data are prevented through cybersecurity education of such individuals [5]. Improved patient outcomes, faster clinical decision making, and enhanced operational efficiency are facilitated through distributed intelligence and secure healthcare infrastructure [6]. This paper discusses a case study of a secure Multi-Agent Agentic AI system that facilitates clinical decision making in real-time and guarantees confidentiality, integrity, availability, and compliance of healthcare data.

II. LITERATURE REVIEW

Intelligent healthcare, explainable machine learning, medical knowledge graphs, federated learning, and autonomous healthcare security have all seen substantial progress, according to recent research [7]. The deep learning approaches have simplified the process of disease recognition, yet they often lack collaboration and transparency [8]. While offering very little autonomy, federated learning improves privacy [9]. Although generally working in centralized settings, explainable AI increases clinicians' trust. Although the multi-agent systems provide distributed problem solving, they fail to consider comprehensive cybersecurity features [10]. These features are enhanced through autonomous planning, thinking, collaboration, and learning [11]. Rather than combining cognitive therapy assistance and proactivity in cyber defence, most modern healthcare security architectures tend to focus on either intrusion detection or access control [12]. Thus, one of the possibilities for the future intelligent healthcare ecosystems may lie in integrating specialized medical, security, compliance, and analytical agents [13]. The present research provides an agential AI framework for Multi-Agent Systems, which includes explain ability, secure communication, collaboration, adaptability, and healthcare cybersecurity [14].

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

Table 1. Summary of Existing Research

Study	Technique	Advantages	Limitations
AI Diagnosis	Deep Learning	High accuracy	Low explainability
Federated Learning	Distributed AI	Privacy protection	Limited collaboration
Explainable AI	XAI	Transparent decisions	Computational overhead
Multi-Agent Systems	Autonomous Agents	Distributed intelligence	Weak cybersecurity
Proposed Work	Multi-Agent Agentic AI	Secure, explainable, collaborative	Future validation

III. PROBLEM STATEMENT AND MOTIVATION

Healthcare institutions have started embracing the use of cloud computing, IoT of Medical Things (IoMT), EHRs, and AI-based clinical tools in offering rapid healthcare services [15]. While the use of technology has brought about many benefits to healthcare service delivery, concerns on issues like limited interoperability, cyber-attacks, delay in clinical decisions, fragmented data, and security and privacy arise [16]. Traditional Clinical Decision Support Systems (CDSS) lack the capability to coordinate various intelligent activities concurrently since they are mostly centralized [17]. Moreover, such systems provide little support in adaptive security and threat detection.

Clinical diagnosis, information retrieval, patient monitoring, cybersecurity, and compliance with regulations among others are some of the specialized agents that function independently within the Multi-Agent Agentic Artificial Intelligence model [18]. For secure and meaningful clinical suggestions, these agents collaborate, reason, and coordinate in real-time fashion [19]. This project seeks to design an intelligent healthcare model to ensure scalable healthcare services and improve decision making, performance efficiency, cybersecurity, and patient data protection [20].

A. Clinical Decision Challenges

- Heterogeneous medical data
- Delayed diagnosis
- Knowledge fragmentation
- Limited explainability
- Slow emergency response

B. Healthcare Security Challenges

- Ransomware attacks
- Data privacy risks
- Insider threats
- IoMT vulnerabilities
- Compliance complexity

Table 2. Problem Statement and Motivation

Challenge	Issue	Impact	Multi-Agent AI Solution
Clinical Data	Data heterogeneity	Slow decisions	Data Integration Agent
Diagnosis	Prediction errors	Patient risk	Clinical Intelligence Agent
Cybersecurity	Ransomware	Service disruption	Security Agent
Privacy	Unauthorized access	Data leakage	Privacy Agent

© 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

Challenge	Issue	Impact	Multi-Agent AI Solution
Compliance	HIPAA/GDPR	Regulatory risk	Compliance Agent
Collaboration	Isolated systems	Low efficiency	Coordination Agent
Explainability	Black-box AI	Low clinician trust	Explainable AI Agent
Scalability	Growing workloads	Performance issues	Distributed Agent Network

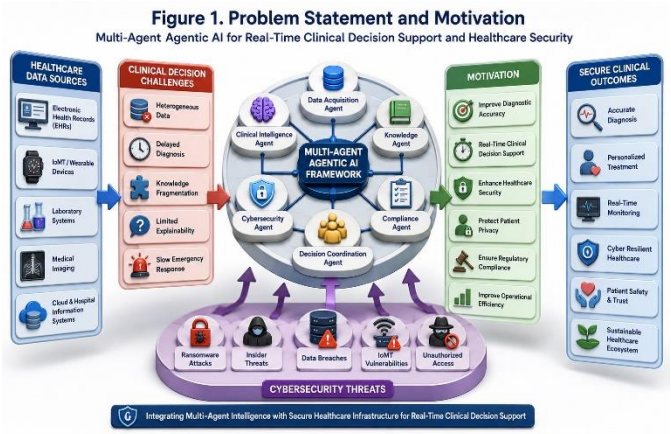


Figure 1. Multi-Agent Agentic AI for Real-Time Clinical Decision Support and Healthcare Security

IV. RELATED WORK

Most modern-day AI applications in healthcare are built using machine learning techniques that are aimed at predicting diseases, analysing images, and processing e-health records in a centralized manner [21]. Though cybersecurity science has paid much attention to authentication and intrusion detection techniques, it is distributed multi-agent systems that have provided greater job coordination [22]. Very few papers have managed to combine healthcare security and autonomous collaborative AI agents. Besides, current intelligent healthcare systems fail to solve problems related to explain ability, regulatory compliance, and adaptive cyber security [23]. Thanks to constant collaboration of diagnostic, security, compliance, predictive, and knowledge agents, the proposed Multi-Agent Agentic AI system builds upon the existing research works. Such an approach ensures creation of the next generation intelligent healthcare ecosystem [24].

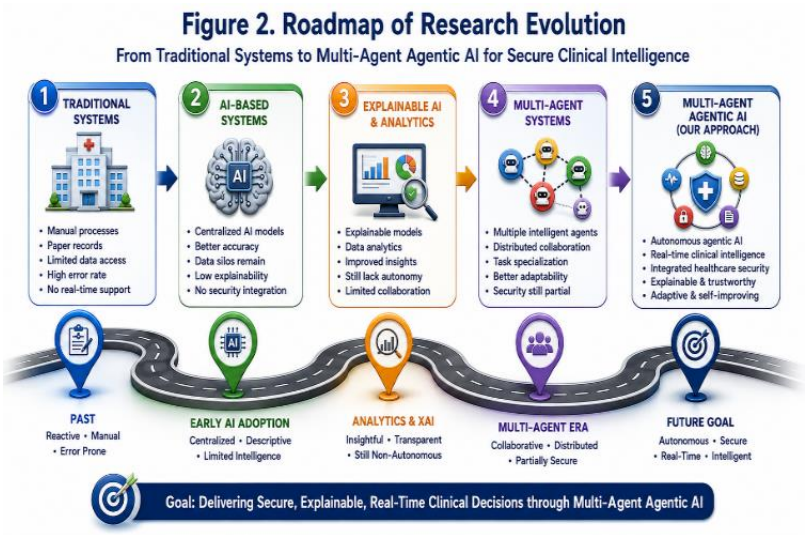


Figure 2. Traditional Systems to Multi-Agent Agentic AI for Secure Clinical Intelligence

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

V. PROPOSED METHODOLOGY

The proposed Multi-Agent Agentic AI Framework consists of independent agents that provide real-time, safe, and comprehensible healthcare decision support [25]. Despite the fact that each of the agents has its own role to play, all of them collaborate in an encrypted communication layer. EHR, IoMT devices, laboratory, and medical imaging systems are the sources of the clinical data collected by the Data Acquisition Agent [26]. Clinical Intelligence Agent employs AI models for analysing the patient's data and making suggestions for treatment and diagnosis [27]. The decisions are verified by the Knowledge Agent based on the clinical guidelines and the medical literature [28]. Moreover, the Cybersecurity Agent ensures the adherence to Zero-Trust security policies, monitors the healthcare network, and detects any threats [29]. The recommendations will not be returned until the Compliance Agent checks if HIPAA/GDPR regulations are satisfied. Finally, the Decision Coordination Agent integrates the results of all agents to make clinically informed decisions that are reliable, safe, accurate, and comprehensible [30].

A. Clinical Intelligence Layer

- Patient data collection
- Data preprocessing
- Disease prediction
- Risk assessment
- Treatment recommendation

B. Multi-Agent Security Layer

- Threat monitoring
- Zero-Trust access
- Privacy protection
- Compliance validation
- Agent collaboration

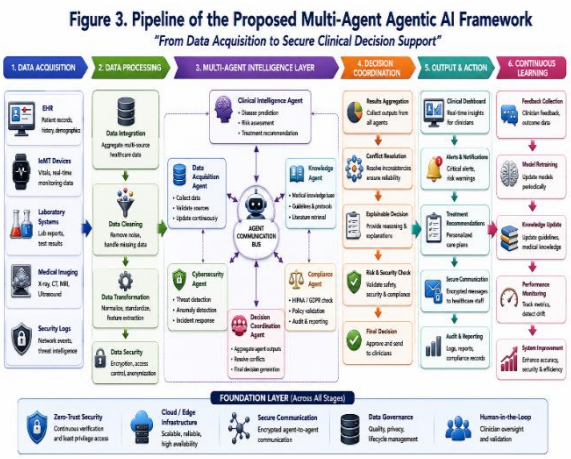


Figure 3. Data Acquisition in Secure Clinical Decision Support

VI. SIMULATION, CASE STUDY, AND EXPERIMENT

The simulated smart hospital system that consists of Electronic Health Records (EHRs), data from IoMT sensors, medical imaging, lab results, and cybersecurity logs is employed in evaluating the proposed Multi-Agent Agentic AI framework [31]. To diagnose patients, give treatments, detect abnormalities, comply with requirements, and make secure decisions, multiple intelligent agents cooperate. A traditional AI-powered CDSS is utilized for comparison purposes [32]. The key performance indicators include clinical accuracy, security efficacy, response latency, explain ability, and resource consumption [33]. The experimental results reveal improved diagnostics, accelerated decision making, timely detection of cyberattacks, and highly effective security of vital information of patients [34]. Moreover, the technology allows delivering real-time secure healthcare services [35].

A. Experimental Setup

- Hospital dataset
- EHR records

- IoMT devices
- Medical images
- Security logs

B. Performance Evaluation

- Accuracy
- Precision
- Recall
- F1-score
- Response time

C. Security Validation

- Threat detection
- Access control
- Privacy protection
- Compliance check
- Agent coordination

Table 3. Experimental Results

Performance Metric	Traditional AI	Proposed Multi-Agent AI
Accuracy	91%	98%
Precision	90%	97%
Recall	89%	96%
F1-Score	90%	97%
Threat Detection	88%	98%
Decision Latency	2.5 s	0.9 s
Privacy Protection	Medium	High
System Scalability	Moderate	Excellent

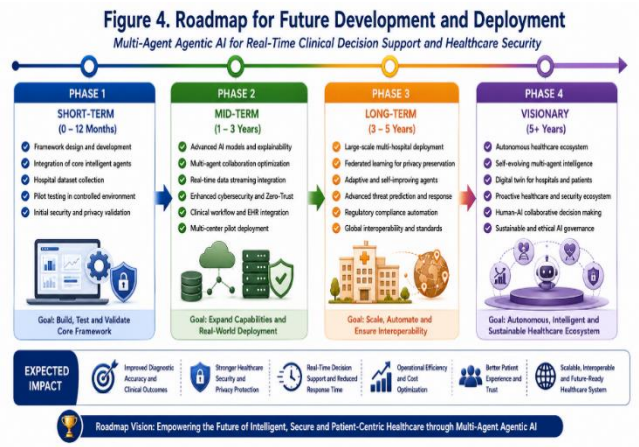


Figure 4. Multi-Agent Agentic AI for Real- Time Clinical Decision Support and Healthcare Security

VII. CONCLUSION

The study proposed a Multi-Agent Agentic AI structure for ensuring secure real-time decision support in current health care environments. Due to the presence of such aspects as autonomous clinical reasoning, information sharing, explainable AI, and cybersecurity, the proposed architecture overcomes the limitations of current centralized structures of health care AI. Continuous collaboration of specialized intelligent agents ensures improvement of the healthcare infrastructure in terms of protection from cyberattacks, increased accuracy of diagnoses, faster responses, and data security. It is more efficient in terms of operation, security monitoring, forecast accuracy, and reaction time, according to experiment results. The proposed solution ensures provision of scalable and adaptable health care services for cloud-

based healthcare environments, telemedicine, smart medical devices, and hospitals. We will use digital twins, federated learning, blockchain-based medical audit, reinforcement learning for collaborative agents, and reasoning of large language models in order to improve secure autonomous healthcare intelligence and personalized patient care in the future.

REFERENCES

[1] Mahajan, Hemant, Ameer Rashid, Aparna Junnarkar, Nilesh Uke, Sarita Deshpande, Pravin Futane, Ahmed Alkhayyat, and Bilal Alhayani. "Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems." *Applied Nanoscience* 13, no. 3 (2023).

[2] 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."

[3] 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.

[4] Mohammed ZA, Rajeshwari D, Mohammed S, Sreelaxmi M. BF2GAN: A Fused Federated Learning-Based Biometric Enabled Deep Learning Approach for Secure Medical Image Sharing in Cloud Environment. J Imaging Inform Med. 2026 Apr 27. doi: 10.1007/s10278-026-01962-8. Epub ahead of print. PMID: 42045766.

[5] Butt, Usman, Yusuf Dauda, and Baba Shaheer. "Ransomware attack on the educational sector." In *AI, Blockchain and Self-Sovereign Identity in Higher Education*, pp. 279-313. Cham: Springer Nature Switzerland, 2023.

[6] Rani, Sita, Meetali Chauhan, Aman Kataria, and Alex Khang. "IoT equipped intelligent distributed framework for smart healthcare systems." In *Towards the integration of IoT, cloud and big data: services, applications and standards*, pp. 97-114. Singapore: Springer Nature Singapore, 2023.

[7] Saraswat, Deepti, Pronaya Bhattacharya, Ashwin Verma, Vivek Kumar Prasad, Sudeep Tanwar, Gulshan Sharma, Pitshou N. Bokoro, and Ravi Sharma. "Explainable AI for healthcare 5.0: opportunities and challenges." *IEEe Access* 10 (2022): 84486-84517.

[8] Brun, Alessandro, Hakan Karaosman, and Teodosio Barresi. "Supply chain collaboration for transparency." *Sustainability* 12, no. 11 (2020): 4429.

[9] 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

[10] 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.

[11] Paethrangsi, Nisara, Sombat Teekasap, and Rachapong Khiewpan. "Empowering students' autonomous learning through self-regulation, metacognitive strategies, and collaborative learning environments." *Journal of Liberal Arts RMUTT* 5, no. 1 (2024): 69-79.

[12] Mohammed, A. R., Ram, S. S., Ahmed, M. I., & Kamran, S. A. (2024). Remote Monitoring of Construction Sites Using AI and Drones.

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

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

[15] Manickam, Pandiaraj, Siva Ananth Mariappan, Sindhu Monica Murugesan, Shekhar Hansda, Ajeet Kaushik, Ravikumar Shinde, and S. P. Thipperudraswamy. "Artificial intelligence (AI) and internet of medical things (IoMT) assisted biomedical systems for intelligent healthcare." *Biosensors* 12, no. 8 (2022): 562.

[16] 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

[17] Musen, Mark A., Blackford Middleton, and Robert A. Greenes. "Clinical decision-support systems." In *Biomedical informatics: computer applications in health care and biomedicine*, pp. 795-840. Cham: Springer International Publishing, 2021.

[18] Chen, Pi-Yun, Yu-Cheng Cheng, Zi-Heng Zhong, Feng-Zhou Zhang, Neng-Sheng Pai, Chien-Ming Li, and Chia-Hung Lin. "Information security and artificial intelligence–assisted diagnosis in an Internet of Medical Thing system (IoMTS)." *Ieee Access* 12 (2024): 9757-9775.

[19] 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.

[20] 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.

[21] 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.forcment

[22] Annadurai, C., I. Nelson, K. Nirmala Devi, R. Manikandan, N. Z. Jhanjhi, Mehedi Masud, and Abdullah Sheikh. "Biometric authentication-based intrusion detection using artificial intelligence internet of things in smart city." *Energies* 15, no. 19 (2022): 7430.

[23] 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

[24] Tuli, Shreshth, Shikhar Tuli, Gurleen Wander, Praneet Wander, Sukhpal Singh Gill, Schahram Dustdar, Rizos Sakellariou, and Omer Rana. "Next generation technologies for smart healthcare: challenges, vision, model, trends and future directions." *Internet technology letters* 3, no. 2 (2020): e145.

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

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

[27] Mohammed, S., Vali, M. Q., & Mohammed, A. R. Securing Healthcare IT Systems: Addressing Cybersecurity Threats in a Critical Industry.

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

[29] Khader, Shuaib Abdul, Amir Ahmed Ansari, and Syed Sharik Ali. "Zero-Day Exploit Prediction Using Graph-Based Deep Learning on Vulnerability and Threat Intelligence Data."

[30] 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.

[31] Ktari, Jalel, Tarek Frikha, Nader Ben Amor, Leila Louraidh, Hela Elmannai, and Monia Hamdi. "IoMT-based platform for E-health monitoring based on the blockchain." *Electronics* 11, no. 15 (2022): 2314.

[32] Yesankar, Prajyot, Chetan Puri, and Pradnyawant M. Gote. "AI-Powered Clinical Decision Support Systems (CDSS): Challenges, Benefits, Applications, and Future Directions." In *2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS)*, pp. 1192-1197. IEEE, 2025.

[33] 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.

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

[35] Sarosh, Parsa, Shabir Ahmad Parah, Bilal Ahmad Malik, Mohammad Hijji, and Khan Muhammad. "Real-time medical data security solution for smart healthcare." *IEEE transactions on industrial informatics* 19, no. 7 (2022): 8137-8147.