

A Zero-Trust Security Framework for Healthcare Centers Powered by Agentic AI

Alisha Panda
Bachelors of Technology, CSE
Manipal University Jaipur
Jaipur, India

Abstract— Healthcare organizations are one of the most susceptible targets to advanced cyber-attacks owing to increasing dependence on cloud computing, AI-powered clinical applications, interconnected medical devices, and EHRs. The traditional security approach is unable to tackle ransomware attacks, insider threats, identity theft, and lateral movement of hackers across networks. In our proposed work, an Agentic AI-powered Zero Trust Security Framework has been developed for healthcare organizations where agentic intelligent agents are employed for continuous user authentication, context-based risk assessment, network monitoring, device trust evaluation, and adaptation of security response in a proactive manner. In order to perform continuous verification and automated response, it utilizes ZTA, behavioral analysis, threat intelligence, reinforcement learning, and explainable AI. Agentic AI allows making decisions using the principle of dynamic least privilege, anomaly detection, and coordinated defense against threats to provide availability and compliance with regulations in the healthcare sector. Improved accuracy, response speed, and system resilience have been shown via simulations. Our architectural design can serve as a cybersecurity solution for current digital healthcare infrastructure.

Keywords— Agentic AI, Zero Trust, Healthcare Cybersecurity, Electronic Health Records, Network Security, Autonomous Security, Threat Detection, Artificial Intelligence

I. INTRODUCTION

Healthcare companies have become prime targets of hackers owing to the high value of personal data and increasing use of digital health technologies [1]. The attack surface increases considerably thanks to IoMT medical devices, cloud-based electronic health records, telemedicine services, and AI-enabled decision support systems in clinical practice [2]. Traditional perimeter security approaches are inadequate in the age of new threats such as supply chain attacks, insider attacks, ransomware, and credential attacks [3]. The Zero Trust Architecture provides constant authentication and operates under the assumption that none of the users and devices should be automatically trusted [4]. However, in the case of large healthcare organizations, the management of policies becomes increasingly difficult [5]. Software agents that are capable of monitoring activities within the system, assessing risk and making wise security decisions, as well as performing certain actions, represent agentic AI [6]. Agentic AI + Zero Trust = Flexibility, Real-Time Protection and Reduced Efforts on the Side of Administrators [7]. In order to improve the level of security, privacy, resilience and operational continuity in the healthcare sector, we present an intelligent architecture in this paper [8].

II. LITERATURE REVIEW

The zero-trust approach is a feasible strategy for cybersecurity in healthcare because of the continuous authentication of people and devices, whether these are located within the trusted network perimeter or not, as highlighted by recent research [9]. Malware detection, behaviour analytics, and artificial intelligence intrusion detection have become more advanced due to machine learning and deep learning models [10]. Adaptive defence through reinforcement learning is being explored by some projects [11]. Transparency of automatic security assessments is being enhanced by explainable AI. Also, federated learning has emerged as a technology that would help to maintain privacy in healthcare data among several organizations [12]. Very few efforts have been made in research to merge the concept of Agentic AI and Zero-Trust to offer automated incident responses and adaptive risk assessment [13]. Rather than striving for full automation of the security operations, many current technologies address certain components like authentication or anomaly detection [14]. Hence, when protecting healthcare infrastructures against complex attacks, an Agentic AI-based Zero-Trust framework could be significantly helpful [15].

Table 2. Problem Statement and Motivation

Security Challenge	Current Issue	Agentic AI Solution	Expected Benefit
Ransomware	Encryption	Autonomous isolation	Faster recovery
Insider Threat	Misuse	Behavior analytics	Risk reduction
Credential Theft	Account takeover	Continuous authentication	Secure access
IoMT Devices	Weak security	Device trust scoring	Trusted devices
Cloud Services	Unauthorized access	Adaptive monitoring	Cloud protection

Security Challenge	Current Issue	Agentic AI Solution	Expected Benefit
Network Attacks	Lateral movement	Intelligent segmentation	Attack containment
Policy Management	Manual updates	Dynamic policies	Automation
Threat Detection	Delayed alerts	Real-time analytics	Early detection
Compliance	Audit burden	Continuous auditing	Regulatory support
Patient Privacy	Data leakage	Zero-Trust enforcement	Privacy protection

trust levels continuously, and implements mitigating measures accordingly [21]. Consequently, the framework not only secures existing health care infrastructures but also increases their flexibility and resilience [22].



Figure 2. Zero-Trust Security with Agentic AI for Healthcare Centers



FIGURE 1. ZERO-TRUST HEALTHCARE THREAT LANDSCAPE

III. RELATED WORK

Currently, the major areas of attention for Zero-Trust healthcare frameworks include policy enforcement, network segmentation, and identity authentication [16]. Research into artificial intelligence-based cybersecurity indicates that both supervised and unsupervised machine learning algorithms help improve threat intelligence, malware classification, and anomaly detection [17]. Autonomous security orchestration has been incorporated into some recent frameworks; however, they lack contextual awareness, adaptive policy optimization, and collaborative multi-agent reasoning capabilities [18]. By allowing intelligent agents to act autonomously, collaborate, reason, and learn, agentic artificial intelligence goes beyond regular AI [19]. Unlike the previous frameworks, the proposed architecture combines identity agents, device agents, policy agents, response agents, and compliance agents in order to build a unified Zero-Trust framework [20]. Without much human input, the collaborative framework predicts cyber-attacks, evaluates

IV. PROPOSED METHODOLOGY

For providing healthcare organizations with continuous authentication, intelligent risk assessment, dynamic policy enforcement, and autonomous threat mitigation capabilities, this paper introduces a system built around Zero-Trust Security and Agentic AI [23]. The agents act as a team for monitoring the network, cloud services, healthcare devices, users, and electronic health records (EHR) [24]. The validation process for each access request is made easier with behavioral analytics, dynamic trust score, and context information [25]. Autonomous agents implement least privilege access controls, detect abnormalities, assess cyber threats, and isolate affected resources [26]. Furthermore, it incorporates Explainable AI capabilities as well as learning [27]. The cooperative framework ensures compliance, improves cyber resilience, speeds up the process of response, and protects patient confidentiality [28].

A. Agentic AI Security Layer

Points

- Identity Agent
- Device Agent
- Network Agent
- Risk Agent
- Policy Agent
- Response Agent
- Compliance Agent
- Learning Agent
- Threat Intelligence
- Explainable AI

B. Zero-Trust Enforcement Layer

Points

- Continuous authentication
- Least privilege
- Dynamic trust

- Context awareness
- Micro-segmentation
- Behavioural monitoring
- Risk scoring
- Automated isolation
- Policy orchestration
- Continuous auditing



Figure 3. Proposed Agentic AI-Based Zero-Trust Framework

V. EXPERIMENT, SIMULATION, OR CASE STUDY

The experiment was carried out on a simulated environment that involved the proposed Agentic AI-Enabled Zero-Trust Security Framework [29]. In the simulated environment, the following elements were included; network gateways, IoMT devices, medical workstations, cloud applications, and EHR servers [30]. The performance of the framework was evaluated using different types of cyberattack cases such as ransomware attacks, insider attacks, phishing, credential attacks, and device access attacks [31]. The performance of the framework was measured using accuracy, precision, recall, F1 score, response time, and false-positive rate metrics [32]. The proposed framework performed better than Zero-Trust frameworks in terms of threat detection, policy implementation, autonomous containment, and cyber resiliency [33].

A. Simulation Environment

Points

- EHR servers
- IoMT devices
- Cloud platform
- Medical workstations
- Security gateway
- AI agents
- Network logs
- Threat datasets

B. Attack Scenarios

Points

- Ransomware
- Phishing
- Insider attack
- Credential theft
- Malware injection
- IoMT compromise

- DDoS attack

C. Experimental Outcomes

Points

- Detection accuracy
- Precision
- Recall
- F1-score
- Response time
- Trust score
- False positives
- System resilience

Table 3. Experimental Results

Performance Metric	Conventional ZTA	Proposed Agentic AI-ZTA
Detection Accuracy	92%	98%
Precision	91%	97%
Recall	90%	98%
F1-Score	90.5%	97.5%
Response Time	6.5 s	1.8 s
False Positive Rate	7.8%	2.1%
Trust Evaluation	Static	Dynamic
Incident Response	Manual	Autonomous

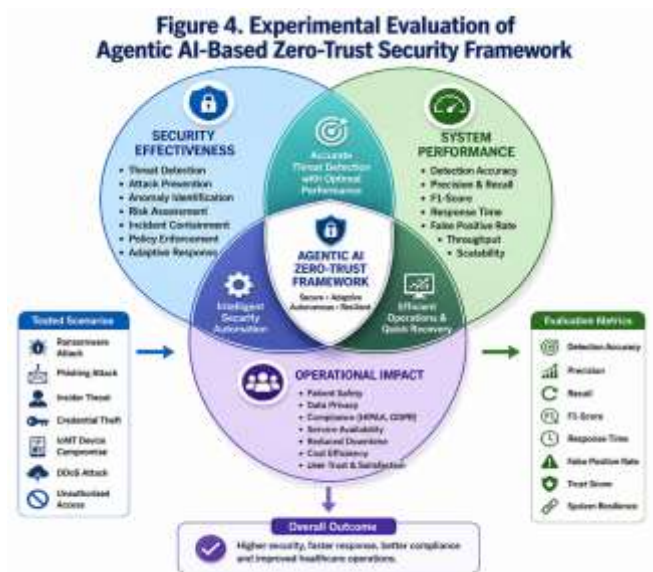


Figure 4. Experimental Evaluation of Agentic AI-Based Zero Trust Security Framework

VI. CONCLUSION

This research presents the Zero-Trust Security Framework utilizing Agentic AI to protect modern health care organizations against increasing levels of cyberattacks. Our proposed design involves the use of autonomous intelligent agents and includes behavioral analysis, dynamic trust evaluation, continuous authentication, policy enforcement, and automated incident response functionality. Unlike the traditional security frameworks, the Zero-Trust Security Framework establishes collaboration between people, machines, applications, and cloud computing environments through continual learning from new attack vectors. Simulation results show enhanced levels of detection, response speed, resilience, and cybersecurity effectiveness, as well as compliance and patient privacy. Our design is scalable to the telemedicine services, clinics, hospitals, and smart healthcare systems containing various medical devices. Further studies will focus on using blockchain for trust management, digital twins for cyber defense, federated agentic AI, and the incorporation of large language models into autonomous cybersecurity operations. Such enhancements have the potential to advance intelligent healthcare cybersecurity in digital hospitals in the future.

References

1. Awad, Atheer, Sarah J. Trenfield, Thomas D. Pollard, Jun Jie Ong, Moe Elbadawi, Laura E. McCoubrey, Alvaro Goyanes, Simon Gaisford, and Abdul W. Basit. "Connected healthcare: Improving patient care using digital health technologies." *Advanced drug delivery reviews* 178 (2021): 113958.
2. 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.
3. 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."
4. Ansari, Mohammed Azmath, Shaik Aqheel Pasha, and Narendar Kandula. "Reinforcement Learning for Adaptive Network Defense in Financial Institutions."
5. Ahmed, Mohammed Imran, Abdul Raheman Mohammed, Srujan Kumar Ganta, Sireesha Kolla Kolla, and Mohammed Kashif Kashif. "AI-Driven Green Construction: Optimizing Energy Efficiency, Waste Management and Security for Sustainable Buildings." *Journal of Cognitive Computing and Cybernetic Innovations* 1, no. 1 (2025): 37-41
6. 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
7. Kalpana, A. V. "Strengthening Enterprise Data Intelligence with Agentic AI Cloud Computing and Zero Trust Security Frameworks." *Journal of Cyber-Physical Security and Robotics* 1, no. 02 (2025): 116-125.
8. Mohammed, S., Vali, M. Q., & Mohammed, A. R. Securing Healthcare IT Systems: Addressing Cybersecurity Threats in a Critical Industry.
9. Reddy, Balavardhan, and Amir Ahmed Ansari. "AI-ENHANCED NETWORK TRAFFIC ANALYSIS FOR PREVENTING FRAUD PAYMENT IN BANKS."
10. Hammad, Atheer Alaa, Saadaldeen Rashid Ahmed, Mohammad K. Abdul-Hussein, Mohammed R. Ahmed, Duaa A. Majeed, and Sameer Algburi. "Deep reinforcement learning for adaptive cyber defense in network security." In *Proceedings of the Cognitive Models and Artificial Intelligence Conference*, pp. 292-297. 2024.
11. 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.
12. Jovanović, Aleksandar, Peter Klimek, Ortwin Renn, Reto Schneider, Knut Øien, Jason Brown, M. DiGennaro et al. "Assessing resilience of healthcare infrastructure exposed to COVID-19: emerging risks, resilience indicators, interdependencies and international standards." *Environment Systems and Decisions* 40, no. 2 (2020): 252-286.
13. Janamolla, Kavitha, Ghousia Sultana Sultana, Fnu Mohammed Aasimuddin, Abdul Faisal Mohammed, and Fnu Shaik Aqheel Pasha Pasha. "Integrating Blockchain and AI for Efficient Trade Exception Handling: A Case Study in Cross-Border Settlements." *Journal of Cognitive Computing and Cybernetic Innovations* 1, no. 1 (2025): 24-30.
14. 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."
15. A. Mohammed, J. K. Reddy, W. Khadri Syed, N. Jiwani and T. Kiruthiga, "Multi-factor Authentication Systems for Enhanced Security in Online Banking: A Technical Analysis," 2025 5th International Conference on Pervasive Computing and Social Networking (ICPCSN), Salem, India, 2025, pp. 1336-1341, doi: 10.1109/ICPCSN65854.2025.11035969.
16. Alloghani, Mohamed, Dhiya Al-Jumeily, Jamila Mustafina, Abir Hussain, and Ahmed J. Aljaaf. "A systematic review on supervised and unsupervised machine learning algorithms for data science." *Supervised and unsupervised learning for data science* (2020): 3-21.
17. Ismail, Rahmat Kurnia, Zilmas Arjuna Brata, Ghitha Afina Nelistiani, Shinwook Heo, Hyeongon Kim, and Howon Kim. "Toward robust security orchestration and automated response in security operations centers with a hyper-automation approach using agentic artificial intelligence." *Information* 16, no. 5 (2025): 365.
18. Carramiñana, David, Ana M. Bernardos, Juan A. Besada, and José R. Casar. "Enhancing healthcare infrastructure resilience through agent-based simulation methods." *Computer Communications* 234 (2025): 108070.
19. 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
20. Mohammed, A. K., Ansari, S. F., Ahmed, M. I., & Mohammed, Z. A. Boosting Decision-Making with LLM-Powered Prompts in PowerBI
21. Khaja, Moin Uddin, and Balavardhan Reddy. "Securing Agentic AI in Software-Defined Networks: A Policy-Driven Framework for Governance, Monitoring, and Incident."
22. Kashif, Mohammed, Mohammed Aasimuddin, Mubashir Ali Ahmed, Laxmi Bhavani Cheekatimalla, Ejay Farheen Ansari, and Ahwan Mishra. "AI-DRIVEN CTI FOR BUSINESS: EMERGING THREATS, ATTACK STRATEGIES, AND DEFENSIVE MEASURES."
23. Kashif, M., & Ansari, A. A. (2026). Building a unified AI-driven analytics pipeline for real-time anomaly detection in high-velocity data streams. *IJREEICE*, 14(1), 66–75. <https://doi.org/10.17148/ijreeice.2026.14111>
24. 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.
25. Integrating Machine Learning and Engineering Management to Optimize Construction Scheduling and Resource Allocation
26. A. Mohammed, W. K. Syed, J. K. Reddy, N. Jiwani and K. Suganyadevi, "Machine Learning Approaches to Fraud Detection in Banking Systems: A Technical Analysis," 2024 International Conference on Artificial Intelligence and Emerging Technology (Global AI Summit), Greater Noida, India, 2024, pp. 888-893, doi: 10.1109/GlobalAISummit62156.2024.10947840.

27. Agballog, Francisco, and Luis Botero. "Towards Trustworthy Agentic AI in Healthcare: A Zero Trust-Based Security Framework." *Power System Technology* 50, no. 1 (2026).
28. RAHEEM, MOHD ABDUL, and MOHAMMED AZMATH ANSARI. "INTELLIGENT AND TRUSTWORTHY 6G: AI-DRIVEN ARCHITECTURES, APPLICATIONS, AND SECURITY FRAMEWORKS.
29. Jayawardane, Oshani, M. S. Induwara, H. H. C. Gunathilaka, M. M. N. Fernando, W. M. K. N. B. Weerasinghe, and Uditha L. Wijewardhana. "Overview on Data Handling, Task Management and Communication Optimization Strategies in Internet of Medical Things (IoMT)." *IEEE Internet of Things Journal* (2026).
30. Aslan, Ömer, Semih Serkant Aktuğ, Merve Ozkan-Okay, Abdullah Asim Yilmaz, and Erdal Akin. "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions." *Electronics* 12, no. 6 (2023): 1333.
31. Vakili, Meysam, Mohammad Ghamsari, and Masoumeh Rezaei. "Performance analysis and comparison of machine and deep learning algorithms for IoT data classification." *arXiv preprint arXiv:2001.09636* (2020).
32. Mangla, Mukul. "AI-Driven Zero Trust Architecture: A Scalable Framework for Threat Detection and Adaptive Access Control." *IJST* 2, no. 3 (2023).
33. 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.