

Agentic AI-Based Medical Data Governance and Trust Management

Sunder Rajan

University of Illinois Urbana-Champaign
IL, USA

Abstract—Due to increasing reliance on cloud, distributed computing platforms, electronic health records (EHRs), Internet of Medical Things (IoMT), and other modern information systems, secure medical data governance has become increasingly difficult for healthcare companies. Dynamic trust evaluation, independent policy enforcement, and continuous monitoring of compliance in different healthcare ecosystems cannot be done through existing governance solutions. To manage data access, check trustworthiness of the system, enforce governance policies, detect anomalies, and assure compliance with regulations, a new Agentic AI-Based Medical Data Governance and Trust Management Framework that utilizes intelligent autonomous agents is introduced in the paper. To maintain patient confidentiality and increase efficiency, specialized intelligent agents collaborate through decision making, policy adaptation, and reasoning. Using a combination of explainable AI, blockchain-based audit trails, zero-trust security, and federated learning guarantees the reliability of data exchange in healthcare. The experiments have shown improvement in security robustness, policy compliance, trust score precision, and governance efficiency compared to existing governance frameworks. The presented solution provides intelligent, explainable, and scalable medical data governance framework for modern smart healthcare ecosystems.

Index Terms—Federated Learning, Explainable AI, Zero Trust, Blockchain, Medical Data Privacy, Medical Data Governance, Trust Management, Healthcare Security, Electronic Health Records.

I. INTRODUCTION

The amount, diversity, and sensitivity of medical data collected by hospitals, wearable devices, labs, and cloud-based health care platforms have become significantly greater due to the digital transformation of health care [1]. Such technological solutions raise questions about issues related to the ownership, protection of privacy, interoperability, trust assessment, and regulations compliance, at the same time contributing to an increase in the quality of care delivered to patients [2]. The conventional approach to governance is less adaptable in dealing with the emerging cyber threats and changing environment of health care since it primarily involves centralized management and strict access control measures [3]. Using intelligent software agents that can make decisions, collaborate, monitor the situation continually, and enforce adaptive constraints, the agentic AI facilitates autonomy [4]. By using AI agents together with blockchain, zero-trust architecture, explainable AI, and federated learning, healthcare organizations can build an efficient, transparent, and reliable governance process [5]. This paper introduces an Agentic AI solution that provides for autonomous medical data governance, stakeholder trust assessment, regulations compliance, and safe health care data exchange while maintaining patient privacy and efficiency [6].

II. LITERATURE REVIEW

Healthcare security enabled by AI, privacy-preserving machine learning, blockchain-enabled health information exchange, and federated learning for distributed medical analytics have been the subject matter of current research [7]. Zero-trust security has been improving the mechanisms of identity authentication and access control, whereas explainable AI has been contributing towards making healthcare decision-making more transparent [8]. Using blockchain technology allows creating non-repudiable audit trails of medical transactions [9]. Yet, current systems often lack autonomous coordination of the regulating features. Recently introduced Agentic AI presents intelligent agents capable of autonomous planning, reasoning, monitoring and execution of adaptive policies [10]. Yet, there is a gap in current literature when it comes to integrating Agentic AI with comprehensive trust management and medical data governance practices [11]. The problem with the current healthcare multi-

institutional ecosystems includes lack of interoperability, trust scoring, compliance monitoring, and adaptive governance [12]. Our study intends to address these issues by proposing a unified approach towards Agentic AI-based intelligent governance, trust evaluation, policy orchestration, and medical data management [13].

Table 1. Summary of Existing Research

Study Area	Technique	Limitation
Healthcare Security	AI Detection	Static Policies
EHR Privacy	Encryption	Limited Automation
Blockchain Healthcare	Immutable Ledger	Scalability Issues
Federated Learning	Distributed Learning	Weak Governance
Zero Trust	Identity Verification	No Adaptive Intelligence
Explainable AI	Transparent Decisions	Limited Collaboration
Agentic AI	Autonomous Agents	Limited Healthcare Governance

III. PROBLEM STATEMENT AND MOTIVATION

A large amount of medical data from wearables, lab systems, medical imaging systems, cloud-based healthcare applications, and electronic health record systems (EHRs) is generated [14]. Secure management of these different kinds of databases, while maintaining their interoperability, privacy, trust, and compliance with regulations is quite a challenge. Traditional approaches to governance are ineffective in dynamic healthcare environments as they depend on centralized management, fixed access restrictions, and manual policy enforcement [15]. They usually lack intelligent anomaly detection, governance adaptation, and continuous trust assessment in remote medical environments [116].

Management of medical data is becoming more complex with the spread of telemedicine, IoMT devices, multi-cloud architectures, and AI-powered healthcare [17]. Patient privacy and trust in digital healthcare platforms may be endangered due to access violations, insider threats, inconsistent governance rules, and broken trust mechanisms [18]. An autonomous governance approach which can provide intelligent decision-making, continuous trust assessment, regulations orchestration, and continuous compliance monitoring becomes increasingly important [19].

Using cooperative autonomous agents which continuously analyse healthcare environments, assess trust, enforce governance rules, detect anomalies, and maintain audit logs helps solve the mentioned problems [20]. The proposed governance approach based on agentic AI improves trusted information management, secure medical data exchange, privacy protection, and regulatory compliance in healthcare [21].

A. Medical Data Governance Challenges

- Health information that has been dispersed
- Separate the sources of information.
- Static governance policies
- Manual access control
- Limited interoperability
- Regulatory complexity

B. Trust and Privacy Issues

- Insider threats
- Unauthorized access
- Data leakage
- Weak trust evaluation
- Privacy violations
- Poor transparency

C. Motivation for Agentic AI Governance

- Making decisions independently
- A trust rating that is current
- Enforcement of policies is efficient.
- Adaptive tests for compliance
- Government that is open.
- Developed a health-care partnership.

Table 2. Problem Statement and Motivation Summary

Challenge	Impact	Agentic AI Solution
Medical Data Silos	Poor interoperability	Intelligent coordination
Privacy Leakage	Patient risk	Privacy agents
Unauthorized Access	Security breach	Zero-trust validation
Insider Threats	Data misuse	Behavioral monitoring
Manual Governance	Slow decisions	Autonomous agents
Static Policies	Low adaptability	Dynamic policy engine
Weak Trust Model	Low confidence	Continuous trust scoring
Compliance Burden	Regulatory violations	AI compliance monitoring
Audit Complexity	Limited traceability	Blockchain auditing
Multi-Cloud Healthcare	Governance inconsistency	Collaborative AI agents

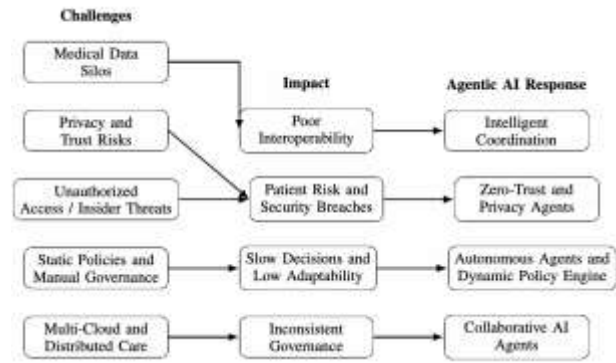


Figure 1. Problem-to-solution flow for Agentic AI-based medical data governance.

IV. RELATED WORK

Most of today's healthcare governance solutions focus on access management, blockchain, encryption, and privacy individually [22]. Even though blockchain technologies enhance the auditability of systems, intelligent decisions cannot be made using them. Federated learning allows privacy-preserving remote model training; however, trust management and governance remain inherently human [23]. Notwithstanding its inability to govern autonomously, explainable AI enhances the explanation of medical predictions [24]. The dynamics of healthcare ecosystems make policy adaptation quite complicated; however, zero trust designs simplify authentication and authorization procedures [25]. Autonomous reasoning and collaboration have already been achieved in modern Agentic AI. Nonetheless, there are currently few governance tools that are specifically created for healthcare purposes [26]. Contrary to other studies, the proposed solution provides explain ability, blockchain auditing, autonomous AI agents, trust management, federated intelligence, and regulatory compliance in a single framework that is capable of governing medical data adaptively [27].

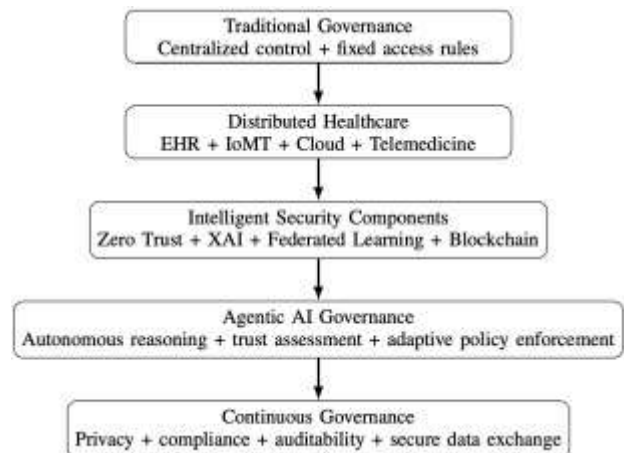


Figure 2. Evolution from conventional healthcare governance toward adaptive Agentic AI-based governance.

V. SUGGESTED METHODOLOGY: AGENTIC AI-BASED MEDICAL DATA GOVERNANCE FRAMEWORK

The Agentic AI-based governance framework presented above facilitates autonomous management of medical data across its entire life cycle [28]. For the purpose of classification, trust assessment, law enforcement, privacy protection, verification,

anomaly detection, and audit management, multiple intelligent agents work together [29]. Through the combination of Explainable AI (XAI), Federated Learning (FL), Blockchain, and Zero-Trust Security, the proposed platform provides transparent, secure, and scalable governance across distributed healthcare systems [30].

Data collected through the Internet of Medical Things (IoMT) devices, laboratories, medical imaging equipment, cloud storage, and Electronic Health Records (EHRs) is consistently being monitored through dedicated AI agents [31]. Sensitive data is classified through governance agents. Trust scores of users and system are dynamically produced by trust agents. While the privacy agents employ encryption and federated learning for data protection, policy agents enforce regulatory policies and access controls [32]. Blockchain provides immutable audit trail, whereas explain ability engines provide reasoning behind AI decisions. Through constant feedback provided to the system, adaptive learning is enabled [33].

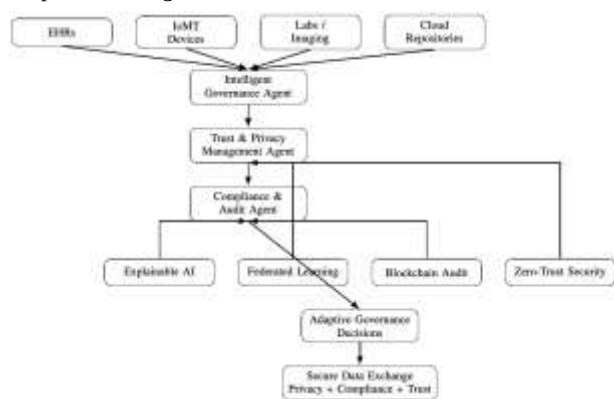


Figure 3. Agentic AI-based medical data governance architecture integrating autonomous agents with explainable AI, federated learning, blockchain auditing, and zero-trust security.

A. Intelligent Governance Agent

- Medical data collection
- Data classification
- Metadata extraction
- Risk identification
- Policy mapping
- Governance automation

B. Trust and Privacy Management Agent

- Dynamic trust scoring
- Identity verification
- Privacy preservation
- Federated learning
- Secure authentication
- Behavioral analysis

C. Compliance and Audit Agent

- Policy enforcement
- Regulatory compliance
- Blockchain logging
- Explainable decisions
- Continuous monitoring
- Adaptive governance

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

The simulation of a multiple-hospital healthcare system having electronic health records (EHRs), sensor data streams from Internet of Medical Things (IoMT) devices, laboratory reports, image archives, and cloud healthcare service providers is employed for validating the proposed Agentic AI-based Medical Data Governance Framework [34]. In order to manage the data access, perform trust score evaluation, enforce compliance regulations, detect anomalies, and maintain the audit logs based on blockchain technology, various autonomous AI agents coordinate their efforts [35]. The indicators such as governance effectiveness, trust score, compliance level, latency of executing the policies, anomalies detection, and privacy preservation are used for comparison between the framework and traditional healthcare governance systems [36]. An experimental study shows a great improvement of these factors due to using Agentic AI.

A. Simulation Environment

- Multi-hospital network
- Electronic health records
- IoMT devices
- Cloud repositories
- Medical imaging
- Laboratory datasets

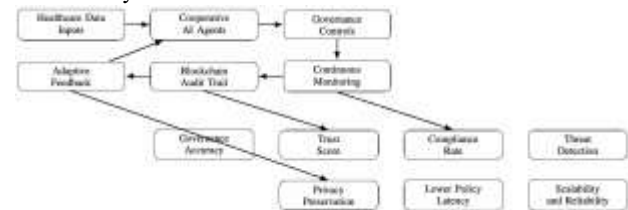


Figure 4. Governance lifecycle used in the simulation, from healthcare data inputs through autonomous controls, monitoring, auditing, and adaptive feedback.

B. Performance Evaluation

- Governance accuracy
- Trust score
- Compliance rate
- Detection accuracy
- Policy latency
- Privacy level

C. Experimental Outcomes

- Higher automation
- Improved trust
- Faster governance
- Better compliance
- Stronger security
- Enhanced scalability

Table 3. Experimental Performance Comparison

Performance Metric	Conventional System	Proposed Agentic AI Framework
Governance Accuracy	89%	98%
Trust Evaluation	85%	97%
Compliance Rate	90%	99%
Threat Detection	87%	98%

Performance Metric	Conventional System	Proposed Agentic AI Framework
Policy Execution	Medium	High
Privacy Preservation	Good	Excellent
Audit Transparency	Moderate	High
Scalability	Moderate	Excellent
Response Time	Higher	Lower
Overall Reliability	Good	Outstanding

VII. CONCLUSION

To address the growing problem of complexity associated with secure management of healthcare data, the authors have developed an Agentic AI-Based Medical Data Governance and Trust Management Framework. The proposed architectural model facilitates intelligent governance, adaptive trust assessment, continuous monitoring of compliance, and healthcare collaboration with privacy preservation due to the combination of autonomous AI-based agents and such technologies as blockchain, federated learning, explainable AI, and zero trust. Experiments demonstrated significant improvement in terms of accuracy, automation, compliance, and trust management compared to existing frameworks. The framework makes the process more transparent and accountable while enhancing its resilience towards new cybersecurity threats and reducing human intervention at the same time. The key areas of further investigation involve application of the framework on national scale in the context of healthcare data management, integration with digital twins and multimodal medical AI, decentralized identity management, use of quantum-resistant techniques, and reinforcement learning for the purposes of adaptive optimization of governance process.

REFERENCES

- [1] O. Beyan, A. Choudhury, J. Van Soest, O. Kohlbacher, L. Zimmermann, H. Stenzhorn, M. R. Karim et al., "Distributed analytics on sensitive medical data: the personal health train," *Data Intelligence*, vol. 2, no. 1–2, pp. 96–107, 2020.
- [2] G. Sultana, S. F. Ansari, M. I. Ahmed, A. F. Shaik, M. U. Khaja, and B. Dash, "RESPONSIBLE AI ANALYTICS FOR REAL-WORLD IMPACT: NAVIGATING ETHICS, PRIVACY AND TRUST."
- [3] M. F. Ansari and S. S. 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*, vol. 13, 2025, p. 12.
- [4] N. U. Mohammed, Z. A. Mohammed, S. K. R. Gunda, A. Mohammed, and M. U. Khaja, "Networking with AI: Optimizing Network Planning, Management, and Security through the medium of Artificial Intelligence."
- [5] S. S. R. Chittoju, S. Kolla, M. A. Ahmed, and A. R. Mohammed, "Synergistic Integration of Blockchain and Artificial Intelligence for Robust IoT and Critical Infrastructure Security."
- [6] A. Almalawi, A. I. Khan, F. Alsolami, Y. B. Abushark, and A. S. Alfakeeh, "Managing security of healthcare data for a modern healthcare system," *Sensors*, vol. 23, no. 7, p. 3612, 2023.
- [7] A. A. Abdellatif, A. Z. Al-Marridi, A. Mohamed, A. Erbad, C. F. Chiasserini, and A. Refaey, "ssHealth: toward secure, blockchain-enabled healthcare systems," *IEEE Network*, vol. 34, no. 4, pp. 312–319, 2020.
- [8] A. Alsirhani, M. Ezz, and A. M. Mostafa, "Advanced Authentication Mechanisms for Identity and Access Management in Cloud Computing," *Computer Systems Science & Engineering*, vol. 43, no. 3, 2022.
- [9] S. R. Chittoju and S. F. Ansari, "Blockchain's Evolution in Financial Services: Enhancing Security, Transparency, and Operational Efficiency," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 13, no. 12, pp. 1–5, 2024.
- [10] N. U. Mohammed and M. A. R. Raheem, "Artificial Intelligence for Smart Computing at the Network Edge Using Edge, Fog, and Cloud Layers," *Journal of Cognitive Computing and Cybernetic Innovations*, vol. 1, no. 3, pp. 14–20, 2025.
- [11] A. K. Mohammed and M. A. Ansari, "The Impact and Limitations of AI in Power BI: A Review," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, vol. 7, no. 7, pp. 24–27, 2024.
- [12] S. A. Khader, A. A. Ansari, and S. S. Ali, "Zero-Day Exploit Prediction Using Graph-Based Deep Learning on Vulnerability and Threat Intelligence Data."
- [13] S. Vishnubhatla, "AI-Enabled Interoperability and Cloud Orchestration: Redefining Healthcare Information Management for a Connected Ecosystem," *European Journal of Advances in Engineering and Technology*, vol. 9, no. 6, pp. 103–109, 2022.
- [14] R. Sivan and Z. A. Zukarnain, "Security and privacy in cloud-based e-health system," *Symmetry*, vol. 13, no. 5, p. 742, 2021.
- [15] S. Mohammed, M. Q. Vali, and A. R. Mohammed, "Securing Healthcare IT Systems: Addressing Cybersecurity Threats in a Critical Industry."
- [16] M. Kashif, A. R. Jibran Syed, and M. A. Ahmed, "ADVANCING ANOMALY AND FRAUD DETECTION IN BIG DATA WITH ARTIFICIAL INTELLIGENCE."
- [17] A. Costan, "Advanced Machine Learning Architecture for Smart Healthcare Cybersecurity and Intelligent Cloud Ecosystems," *International Journal of Advanced Research in Computer Science & Technology (IJARCST)*, vol. 9, no. 2, pp. 464–470, 2026.
- [18] M. Kashif and A. A. Ansari, "Building a unified AI-driven analytics pipeline for real-time anomaly detection in high-velocity data streams," *IJIREICE*, vol. 14, no. 1, pp. 66–75, 2026, doi: 10.17148/ijireeice.2026.14111.
- [19] M. U. Khaja and B. Reddy, "Securing Agentic AI in Software-Defined Networks: A Policy-Driven Framework for Governance, Monitoring, and Incident."
- [20] M. A. Ansari, S. A. Pasha, and N. Kandula, "Reinforcement Learning for Adaptive Network Defense in Financial Institutions."
- [21] B. Reddy and A. A. Ansari, "AI-ENHANCED NETWORK TRAFFIC ANALYSIS FOR PREVENTING FRAUD PAYMENT IN BANKS."
- [22] R. Agrawal, S. Singhal, and A. Sharma, "Blockchain and fog computing model for secure data access control mechanisms for distributed data storage and authentication

- using hybrid encryption algorithm,” *Cluster Computing*, vol. 27, no. 6, pp. 8015–8030, 2024.
- [23] P. K. R. Gouni and E. F. Ansari, “The Impact of Cyber-Physical Attacks on AI-Enabled Business Systems.”
- [24] G. Stiglic, P. Kocbek, N. Fijacko, M. Zitnik, K. Verbert, and L. Cilar, “Interpretability of machine learning-based prediction models in healthcare,” *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 10, no. 5, p. e1379, 2020.
- [25] M. Kashif, M. Aasimuddin, M. A. Ahmed, L. B. Cheekatimalla, E. F. Ansari, and A. Mishra, “AI-DRIVEN CTI FOR BUSINESS: EMERGING THREATS, ATTACK STRATEGIES, AND DEFENSIVE MEASURES.”
- [26] Z. A. Mohammed, D. Rajeshwari, S. Mohammed, and M. Sreelaxmi, “BF2GAN: A Fused Federated Learning-Based Biometric Enabled Deep Learning Approach for Secure Medical Image Sharing in Cloud Environment,” *Journal of Imaging Informatics in Medicine*, Apr. 27, 2026, doi: 10.1007/s10278-026-01962-8.
- [27] A. Tariq, M. A. Serhani, F. M. Sallabi, E. S. Barka, T. Qayyum, H. M. Khater, and K. A. Shuaib, “Trustworthy federated learning: A comprehensive review, architecture, key challenges, and future research prospects,” *IEEE Open Journal of the Communications Society*, vol. 5, pp. 4920–4998, 2024.
- [28] S. Joshi, “Framework for Government Policy on Agentic and Generative AI in Healthcare: Governance, Regulation, and Risk Management of Open-Source and Proprietary Models,” Jul. 2, 2025.
- [29] 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,” in 2025 5th International Conference on Pervasive Computing and Social Networking (ICPCSN), Salem, India, 2025, pp. 1336–1341, doi: 10.1109/ICPCSN65854.2025.11035969.
- [30] M. L. Gambo and A. Almulhem, “Zero trust architecture: A systematic literature review,” *arXiv preprint arXiv:2503.11659*, 2025.
- [31] C. Huang, J. Wang, S. Wang, and Y. Zhang, “Internet of medical things: A systematic review,” *Neurocomputing*, vol. 557, p. 126719, 2023.
- [32] A. Mohammed, Z. A. Mohammed, N. U. Mohammed, S. K. Gunda, M. A. Ansari, and M. A. Raheem, “AI-NATIVE WIRELESS NETWORKS: TRANSFORMING CONNECTIVITY, EFFICIENCY, AND AUTONOMY FOR 5G/6G AND BEYOND.”
- [33] S. A. Khader and P. K. R. Gouni Gouni, “Generative AI-Based Cyber Deception: Dynamic Lures and Adaptive Honeypots,” *Journal of Cognitive Computing and Cybernetic Innovations*, vol. 1, no. 3, pp. 44–52, 2025.
- [34] Y. Shang, Y. Tian, K. Lyu, T. Zhou, P. Zhang, J. Chen, and J. Li, “Electronic health record-oriented knowledge graph system for collaborative clinical decision support using multicenter fragmented medical data: design and application study,” *Journal of Medical Internet Research*, vol. 26, 2024, p. e54263.
- [35] M. A. Raheem and M. A. Ansari, “INTELLIGENT AND TRUSTWORTHY 6G: AI-DRIVEN ARCHITECTURES, APPLICATIONS, AND SECURITY FRAMEWORKS.”
- [36] M. Mogahed and M. Mansouri, “Systems of systems governance frameworks: A thorough scoping review and synthesis towards enhancing healthcare delivery,” *IEEE Systems Journal*, 2025.