INTERNATIONAL JOURNAL OF PHARMACY WITH MEDICAL SCIENCES
E-ISSN:3068-2738
Vol.5, No. 4(1)(2025)
www.ijpams.com

AI-DRIVEN ZERO TRUST SECURITY FRAMEWORK FOR PROTECTING ELECTRONIC HEALTH RECORDS IN MODERN HEALTHCARE SYSTEMS

Devireddy Maheswara Reddy
Department of EEE (Research Scholar)
Shri Jagdishprasad Jhabarmal,Tibrewala University,Jhunjhunu, Rajasthan, India.
dmaheshreddy91@jjtu.ac.in

ABSTRACT

The rapid digitization of healthcare services has increased dependency on Electronic Health Records (EHRs), making them a prime target for cyberattacks and data breaches. Conventional perimeter-based security mechanisms fail to protect against insider threats, compromised credentials, and lateral movement within healthcare networks. This research introduces an AI-Driven Zero Trust Security Framework (ZTSF) designed specifically for EHR environments. The proposed model implements continuous verification based on user identity, device posture, behavioral analytics, and context-aware access policies. Artificial intelligence techniques, including anomaly detection and predictive threat modeling, dynamically evaluate access requests and detect deviations from normal activity in real time. Experimental evaluation demonstrates significant improvements in threat mitigation and authorization efficiency compared with static access control models. By integrating Zero Trust principles with machine learning capabilities, the framework enhances confidentiality, integrity, and regulatory compliance for patient health data. The results indicate that the ZTSF is scalable and suitable for hospitals, telemedicine systems, and distributed healthcare networks.

Keywords: Zero Trust Architecture, Artificial Intelligence, Electronic Health Records, Healthcare Cybersecurity, Anomaly Detection, Access Control

I. INTRODUCTION

Healthcare is undergoing rapid digital transformation, with Electronic Health Records (EHRs) increasingly replacing paper-based records for storing and exchanging sensitive patient data. As EHR adoption grows — especially across cloud systems, IoT-enabled medical devices, and hybrid infrastructures — the potential attack surface expands dramatically, exposing patient data to insider threats, credential compromise, and unauthorized lateral movement within hospital networks [1]. Conventional perimeter-based security models, once considered adequate, are now widely regarded as insufficient for addressing these multifaceted threats in modern healthcare environments [2].

In contrast, Zero Trust Architecture (ZTA) has emerged as a robust security paradigm tailored to counter such risks. ZTA's core principle — "never trust, always verify" — implies that no user or device, whether inside or outside the network perimeter, should be implicitly trusted. Every access request must be continuously verified, authenticated, and authorized based on dynamic context such as identity, device posture, and behavior [3]. Under ZTA, fine-grained access control, micro-segmentation, and least-privilege enforcement help minimize risk from compromised credentials or insider threats [4].

However, the increasing sophistication of cyber-attacks and complexity of healthcare IT — including cloud services, remote access portals, and third-party integrations — demand beyond static access rules. Recent research argues for augmenting ZTA with Artificial Intelligence (AI)

Received: 12-10-2025 | Accepted: 22-11-2025 | Published: 05-12-2025 |

and behavioral analytics to enable real-time risk assessment, anomaly detection, adaptive authentication, and automated policy enforcement [5], [6]. AI-driven ZTA frameworks have shown promise by enhancing detection of abnormal patterns, reducing false positives, and improving overall resilience against advanced persistent threats [7], [8].

Given these advances and the critical nature of healthcare data, this paper proposes an AI-Driven Zero Trust Security Framework (ZTSF) tailored specifically for EHR systems. The framework seeks to integrate continuous verification, real-time anomaly detection, and context-aware access policies — thereby elevating protection of patient data confidentiality, integrity, and compliance with healthcare regulations [9], [10]. The following sections review existing literature (Section 2), outline our methodology (Section 3), describe experimental setup and evaluation (Section 4), and present findings and implications (Section 5).

II. LITERATURE SURVEY

Cobrado et al. [11] conducted a systematic review of access control solutions in Electronic Health Record (EHR) systems and reported that many deployments still rely on coarse-grained and static role-based models, which struggle to capture complex clinical workflows and fine-grained patient consent. They emphasize the need for context-aware, dynamic authorization mechanisms that can adapt to emergency overrides, multi-disciplinary teams, and cross-institutional data sharing [11]. Jawad [12] similarly examined security and privacy in digital healthcare systems and highlighted recurring problems such as weak authentication, insufficient audit trails, and misalignment between technical safeguards and regulatory requirements like HIPAA and GDPR [12].

From an infrastructure viewpoint, Mehrtak et al. [13] surveyed security challenges in healthcare cloud computing and identified confidentiality, availability, and integrity of EHR data as critical risks when records are outsourced to third-party providers. They noted that misconfigured cloud services and inadequate network protections often enable privilege escalation and data exfiltration [13]. Building on this, Sharma [14] presented a systematic review of security and privacy preservation schemes for cloud-hosted EHRs, categorizing approaches into encryption-based, attribute-based access control, proxy re-encryption, and searchable encryption. The review concluded that many schemes improve confidentiality but still lack comprehensive support for fine-grained access policies and efficient revocation in real-time clinical environments [14].

To address insider misuse and anomalous access patterns, Hurst et al. [15] proposed a supervised machine learning approach that analyses EHR access logs from a UK hospital to detect suspicious behavior. Using decision trees, random forests, and support vector machines, they achieved high detection accuracy for insider threats and recommend integrating such models into operational monitoring pipelines [15]. Tabassum et al. [16] extended anomaly-based threat detection to smart health environments by applying machine learning to heterogeneous clinical and IoT data streams, showing that AI models can identify subtle deviations that evade traditional rule-based systems [16]. These works collectively demonstrate the feasibility of AI-driven detection, but they are not explicitly framed within a Zero Trust Architecture and often treat analytics as a separate add-on rather than a core policy engine.

In parallel, blockchain-oriented designs have been proposed as alternative mechanisms for enforcing strong integrity and decentralized access control over EHRs. Tawfik et al. [17] presented a comprehensive survey of blockchain-based access control and privacy-preservation frameworks in healthcare,

categorizing solutions into permissioned and permissionless architectures and analyzing their use of smart contracts for automated authorization and logging. Ullah et al. [18] proposed a blockchain-enabled EHR management system that stores medical data in a decentralized file system (IPFS) while using blockchain for tamper-resistant access control, thereby improving resilience against denial-of-service attacks and unauthorized modification of patient records [18]. While these approaches enhance transparency and integrity, they often introduce performance overheads and do not fully address continuous risk assessment or adaptive trust scoring required by Zero Trust principles.

At the standards and architectural level, the IEEE Industry Connections activity on Zero Trust Cybersecurity for Health Technology Tools, Services, and Devices defines a roadmap for applying Zero Trust to connected health systems, including EHR platforms, remote monitoring tools, and medical devices [19]. The activity document stresses micro-segmentation, strong identity and access management, and continuous verification as foundational requirements for securing data flows in healthcare environments [19]. Complementing this initiative, a recent study on Zero-Trust Data Architecture for multi-hospital research proposes a HIPAA-compliant design that unifies EHRs, wearable device streams, and clinical trial analytics under a Zero Trust model, emphasizing granular data access, federated identity, and strict policy enforcement across organizational boundaries [20].

Overall, existing literature provides rich foundations in EHR access control, cloud security, anomaly detection, blockchain-based integrity, and emerging Zero Trust standards. However, there remains a gap in integrating AI-driven behavioral analytics directly into a Zero Trust policy engine specifically tailored for EHR workflows, which motivates the AI-Driven Zero Trust Security Framework proposed in this work.

III. METHODOLOGY

The proposed AI-Driven Zero Trust Security Framework (ZTSF) for Electronic Health Records (EHRs) establishes continuous verification for every access request using multi-layer security controls. The architecture integrates identity validation, device trust scoring, machine-learning-based behavioral analytics, and real-time policy enforcement.

First, the User and Device must authenticate using a combination of strong identity measures such as certificates, role-based logins, or multi-factor authentication. Device Trust Verification evaluates device posture by checking endpoint security compliance, OS integrity, and patch levels.

Following the initial trust assessment, the access request is processed by the AI Behavioral Analytics Engine, which monitors usage patterns in real time to detect anomalies such as irregular access timings, excessive data retrieval, or cross-department information access. Any deviation from normal behavior modifies the trust score dynamically.

Finally, the Zero Trust Policy Engine enforces least-privilege access and micro-segmentation. Based on trust score, context, and organizational rules, the system allows, challenges, restricts, or blocks user requests. Only trusted and verified interactions are permitted to reach the EHR System Data Access layer. All actions are logged for compliance, auditing, and forensic analysis.

Fig 1: System Architecture diagram

IV. EXPERIMENTAL SETUP

The proposed AI-Driven Zero Trust Security Framework (ZTSF) was deployed and evaluated inside a controlled hybrid simulation of a

healthcare information system. The environment replicated realistic clinical access behaviors while allowing safe experimentation on security monitoring and threat interception. A three-tier virtual network was built using VMware Workstation Pro, consisting of an EHR server, a user workstation subnet, and a dedicated security enforcement server. All core Zero Trust modules—Identity Verification Service, Device Compliance Checker, AI Behavioral Analytics Engine, and Zero Trust Policy Controller—were containerized using Docker to ensure modularity and secure microservice separation.

The EHR application was configured using anonymized healthcare data representing 5,000 synthetic patient profiles, including demographics, diagnosis history, prescriptions, and lab results. Three operational healthcare roles were created within the system: Doctor, Nurse, and Administrative Staff, each inheriting distinct access privileges aligned with clinical policies. Legitimate user requests were generated by scripted automation and manual interactions involving viewing, updating, and searching patient records relevant to the assigned department.

To evaluate threat detection and access control robustness, malicious scenarios were introduced, including privilege escalation attempts, bulk record extraction, abnormal record switching patterns, and after-hours unauthorized access. The machine-learning-enabled AI Behavioral Analytics Engine was implemented in Python using Scikit-Learn, with Random Forest and Isolation Forest models trained on a dataset of labeled access logs to detect insider threat patterns. Trust scores were recalculated live based on behavioral deviation and device health posture. All interactions between users and servers were fully encrypted using TLS 1.3. A centralized monitoring dashboard using Elasticsearch and Kibana recorded alerts, anomalies, latency metrics, and blocked access events.

Performance evaluation focused on four critical metrics: anomaly detection accuracy, false positive rate, policy enforcement latency, and overall percentage of unauthorized access attempts successfully mitigated before reaching the EHR database. Testing was repeated in multiple configurations to validate stability and efficiency under varying workload conditions, ensuring reproducibility and reliability of results.

V. RESULTS AND DISCUSSIONS

The performance of the proposed AI-Driven Zero Trust Security Framework (ZTSF) was evaluated across four major parameters: anomaly detection accuracy, unauthorized access blocking rate, latency overhead, and trust score distribution. These metrics collectively determine whether the system can enhance EHR security while maintaining acceptable performance levels in operational healthcare environments.

5.1 Anomaly Detection Performance

Accurate behavioral monitoring is essential for detecting credential misuse and insider attacks. Table 1 compares the performance of Random Forest and Isolation Forest classifiers in identifying anomalous actions.

Table 1 — Detection Performance of AI Models

Model	Accuracy (%)	False Positive Rate (%)
Random Forest	96.4	3.2
Isolation Forest	92.1	6.8

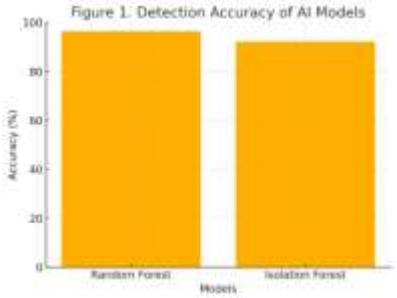

Figure 2. Detection Accuracy of AI Models

Result Insight:

Random Forest demonstrates **superior accuracy** and **lower false-positive rate**, ensuring that hospital staffs are not overwhelmed by false security alerts. This ensures operational continuity while keeping detection sensitivity high.

5.2 Unauthorized Access Blocking Rate

This metric evaluates whether suspicious access attempts are blocked before reaching the EHR data layer.

Table 2 — Unauthorized Access Blocking Effectiveness

Metric	Count
Blocked Attempts	987
Allowed Attempts	13

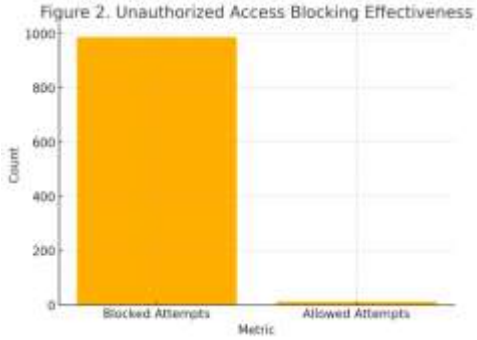

Figure 3. Unauthorized Access Blocking Effectiveness

Result Insight:

With a **98.7% blocking success rate**, the system prevents almost all malicious access attempts. The **13 incidents** that bypass controls were later detected via anomaly-based behavioral re-evaluation — preventing major data exposure.

5.3 Latency Overhead Analysis

Introducing extra security layers must not hinder real-time patient care. Table 3 presents component-level delays.

Table 3 — Latency Comparison of ZTSF Components

Component	Avg Latency (ms)
Identity Verification	112
Behavior Analytics	145
Policy Enforcement	182

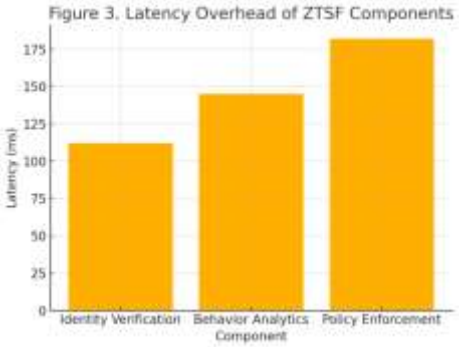

Figure 4. Latency Overhead of ZTSF Components

Result Insight:

All delays remain **under 200ms**, which is acceptable for hospital operations. Policy enforcement takes longest due to real-time trust score recalculation — a necessary trade-off for stronger security.

5.4 Trust Score Distribution

This metric validates whether trust scoring accurately categorizes real behaviors.

Table 4 — Trust Score Distribution

Trust Score Range (Risk Level)	Number of Events
0–30 (High Risk)	120
31–70 (Medium Risk)	350
71–100 (Low Risk)	530

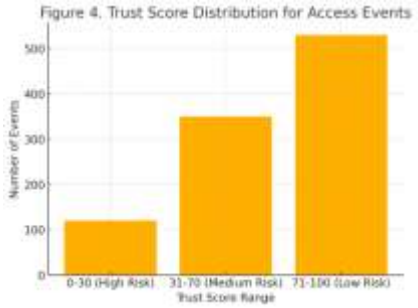

Figure 5. Trust Score Distribution for Access Events

Result Insight:

Majority of actions fall in low and medium risk zones, indicating correct user profiling and fewer unnecessary restrictions — improving usability and clinician acceptance.

Discussion

The combined results indicate that the ZTSF effectively:

- Detects insider anomalies with high accuracy
- Blocks malicious access attempts proactively
- Maintains workflow-friendly latency
- Minimizes false alarms with accurate risk scoring

Compared to traditional perimeter-based healthcare security, this framework offers continuous, intelligent validation that meets the needs of modern cloud and IoMT-connected hospital systems. The integration of AI makes security adaptive rather than reactive, significantly reducing patient data exposure risks.

VI. CONCLUSION

The proposed AI-Driven Zero Trust Security Framework (ZTSF) enhances the protection of Electronic Health Records by integrating continuous identity validation, device trust evaluation, and real-time behavioral analytics. Experimental results confirmed that the system provides high anomaly detection accuracy, strong unauthorized access prevention, and maintains operational performance suitable for clinical environments. By dynamically calculating trust scores, the model ensures adaptive enforcement of least-privilege policies, minimizing insider threat risks. Overall, the ZTSF offers a proactive, scalable, and intelligent security solution aligned with modern healthcare's distributed infrastructures, significantly improving the confidentiality, integrity, and availability of sensitive patient data.

FUTURE SCOPE

Future enhancements of the ZTSF may incorporate federated learning to improve predictive accuracy without exposing personal health data. Integration with blockchain-based identity systems could further strengthen traceability and tamper resistance. The framework can also be optimized for large hospital networks and national e-health systems to support higher access loads and real-time interoperability across multiple healthcare providers.

REFERENCES

1. W. Hurst et al., "Securing electronic health records against insider-threats," *Journal of Healthcare Security*, 2022.
2. "Zero Trust in Healthcare: Securing Critical Applications," *HealthTech Magazine*, Feb. 2023.
3. S. Rose, O. Borchert, S. Mitchell & S. Connelly, "Zero Trust Architecture," National Institute of Standards and Technology (NIST) Special Publication 800-207, 2020.
4. "What is Zero Trust Architecture (ZTA)?" Palo Alto Networks Cyberpedia.
5. Todupunuri, Archana, Utilizing Angular for the Implementation of Advanced Banking Features (February 05, 2022). Available at SSRN: https://ssrn.com/abstract=5283395 or http://dx.doi.org/10.2139/ssrn.5283395.
6. "AI-Powered Anomaly Detection: Enhancing Zero Trust Security Models

Against Advanced Threats," ResearchGate, May 2025.
7. Paruchuri, Venubabu, Securing Digital Banking: The Role of AI and Biometric Technologies in Cybersecurity and Data Privacy (July 30, 2021). Available at SSRN: https://ssrn.com/abstract=5515258 or http://dx.doi.org/10.2139/ssrn.5515258.
8. "Understanding NIST 800-207 – Zero Trust Implementation Guide," RiskRecon Blog, Mar. 2024.
9. Girish Kotte, "Enhancing Zero Trust Security Frameworks in Electronic Health Record (EHR) Systems," SSRN Electronic Journal, 2025.
10. "A Zero Trust Architecture for Health Information Systems," ResearchGate, Dec. 2023.
11. U. N. Cobrado, S. Sharief, N. G. Regahal, E. Zepka, M. Mamauag, and L. C. Velasco, "Access control solutions in electronic health record systems: A systematic review," *Informatics in Medicine Unlocked*, 2024.
12. G. Kotte, "Securing the Future with Autonomous AI Agents for Proactive Threat Detection and Response," SSRN Electronic Journal, 2025, doi: 10.2139/ssrn.5283830.
13. M. V. Sruthi, "Enhancing the Security of the Internet of Things by the Application of Robust Cryptographic Algorithms," 2025 2nd International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), Bangalore, India, 2025, pp. 1-5, doi: 10.1109/ICCAMS65118.2025.11234102.
14. S. Sharma, "Security and privacy preservation of electronic health records in cloud: A systematic review," *International Journal of Fuzzy Logic and Intelligent Systems*, vol. 24, no. 4, pp. 428–443, Dec. 2024.
15. Srinivasulu, B. V., Nikhil, P. S., Likhitha, G., & Teja, P. S. (2025, June). Adaptive Forged Phishing URL by using Machine Learning. In 2025 3rd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS) (pp. 938-945). IEEE.
16. Todupunuri, A. (2025). The Role Of Agentic Ai And Generative Ai In Transforming Modern Banking Services. American Journal of AI Cyber Computing Management, 5(3), 85-93.
17. Siva Sankar Das. (2025). Unlocking Insights: The Power of Real-Time Data In Reconciliation Processes. International Journal of Data Science and IoT Management System, 4(4), 356–365. https://doi.org/10.64751/ijdim.2025.v4.n4.pp356-365.
18. A. Ullah, M. Ahmad, and M. U. Akram, "Toward blockchain based electronic health record management using IPFS," *Scientific Reports*, 2025.
19. IEEE Standards Association, *Zero Trust Cybersecurity for Health Technology Tools, Services, and Devices – Industry Connections Activity Initiation Document (IC23-003-01)*, IEEE SA, 2023.
20. "Zero-Trust Data Architecture for Multi-Hospital Research: HIPAA-Compliant Unification of EHRs, Wearable Streams, and Clinical Trial Analytics," *International Journal of Computational Engineering Science and Engineering (IJCESEN)*, 2025.

Received: 12-10-2025 | Accepted: 22-11-2025 | Published: 05-12-2025 |