International Journal of Information Technology and Electrical Engineering (IJITEE)
ISSN: 2306-708X
Volume 15 Issue 1, January-June, 2026, pp. 7-12.

CROSS-PLATFORM RISK SCORING FOR CLOUD-BASED ELECTRONIC HEALTH RECORDS USING AI-AUGMENTED VULNERABILITY MANAGEMENT

Arina Chimamanda
Cloud Security Analyst, Nigeria.

Bertram Usher Shaw
AI/ML Ops Engineer, Nigeria.

Abstract

As Electronic Health Records (EHRs) increasingly transition to cloud-based infrastructures, the need for robust cybersecurity frameworks becomes paramount. This paper presents an AI-augmented risk scoring model that integrates multi-platform vulnerability management systems to evaluate and mitigate cybersecurity threats in cloud-based EHR systems. By aggregating threat intelligence across operating systems and platforms, the model dynamically assesses risk scores based on real-time exploitability, severity metrics, and asset criticality. A comprehensive review of existing literature, an AI-driven scoring algorithm, and a prototype implementation are discussed, showcasing the model's effectiveness in reducing the mean time to detect (MTTD) and mean time to respond (MTTR) to EHR vulnerabilities. The study contributes to the development of proactive, adaptive defense mechanisms that are platform-agnostic and scalable across heterogeneous healthcare environments.

Keywords: AI risk scoring, Cloud EHR, Vulnerability management, Cybersecurity, Threat modeling, Cross-platform integration, Health informatics security.

Citation: Arina Chimamanda, Bertram Usher Shaw. (2026). Cross-Platform Risk Scoring for Cloud-Based Electronic Health Records Using AI-Augmented Vulnerability Management. *International Journal of Information Technology and Electrical Engineering (IJITEE)*, 15(1), 7–12.

1. INTRODUCTION

The healthcare sector's digital transformation has increased reliance on cloud-based platforms to manage Electronic Health Records (EHRs). While cloud infrastructure enhances accessibility and scalability, it also expands the attack surface for cyber threats. The rise of ransomware attacks, phishing, and zero-day vulnerabilities targeting EHRs highlights the urgency of developing robust, intelligent security frameworks. Traditional static vulnerability scanners fail to adapt to evolving threats across multiple platforms. This necessitates a risk scoring system capable of synthesizing dynamic threat intelligence and contextual asset information.

Artificial Intelligence (AI) offers promising solutions in automating and enhancing the detection and mitigation of threats. By embedding AI within vulnerability management frameworks, healthcare providers can proactively evaluate security postures, optimize resource allocation, and reduce human error. This study introduces a novel AI-augmented risk scoring approach tailored for cross-platform cloud-based EHR systems, combining severity metrics (e.g., CVSS), exploit probability, and system interdependencies. Through a prototype system and experimental evaluation, we demonstrate how our model enhances threat detection and decision-making in real time.

2. LITERATURE REVIEW

Recent literature highlights growing interest in automated and AI-based vulnerability management in healthcare IT systems. Wang et al. (2023**)** proposed a deep learning model for vulnerability classification in cloud environments, demonstrating improved precision in identifying high-risk CVEs. Their study underscored the limitations of static rule-based systems in dynamic cloud ecosystems). Patel and Morris (2022**)** explored AI-driven risk assessment for healthcare IoT networks, revealing that real-time data correlation significantly improves attack detection rates.

Further, Lopez and Cheng (2024) implemented a cross-platform vulnerability scanner integrating Bayesian networks to predict threat propagation in hybrid cloud infrastructures Their model provided probabilistic inference of breach likelihoods, highlighting the benefits of multi-source intelligence. Agarwal et al. (2023**)** developed a framework using reinforcement learning to optimize patch management across virtualized health systems These approaches inform our proposed architecture, integrating AI-based scoring and cross-platform asset awareness.

3. METHODOLOGY AND MODEL ARCHITECTURE

Our proposed framework integrates vulnerability feeds (e.g., NVD, CISA KEVs), platform-specific telemetry (Windows, Linux, containerized systems), and asset metadata (e.g., EHR application tier) into a centralized AI risk engine. The risk scoring pipeline consists of preprocessing, feature extraction, AI-based classification, and weighted scoring.

$$\text{Risk Score} = \alpha \cdot \text{CVSS}_{\text{base}} + \beta \cdot \text{Exploitability} + \gamma \cdot \text{Asset Impact}$$

Where weights (α, β, γ) are optimized via supervised learning using incident response datasets.

The architecture is depicted in the following

3.1 Data Collection and Preprocessing

The system collects real-time vulnerability data from trusted sources such as the National Vulnerability Database (NVD), CISA Known Exploited Vulnerabilities (KEV) catalog, and internal threat feeds. Each vulnerability entry is matched with corresponding cloud-based EHR assets based on system metadata and deployment context. Natural language processing (NLP) techniques are used to extract relevant features from unstructured vulnerability descriptions. This structured data serves as input for the AI classification and scoring modules in the later pipeline.

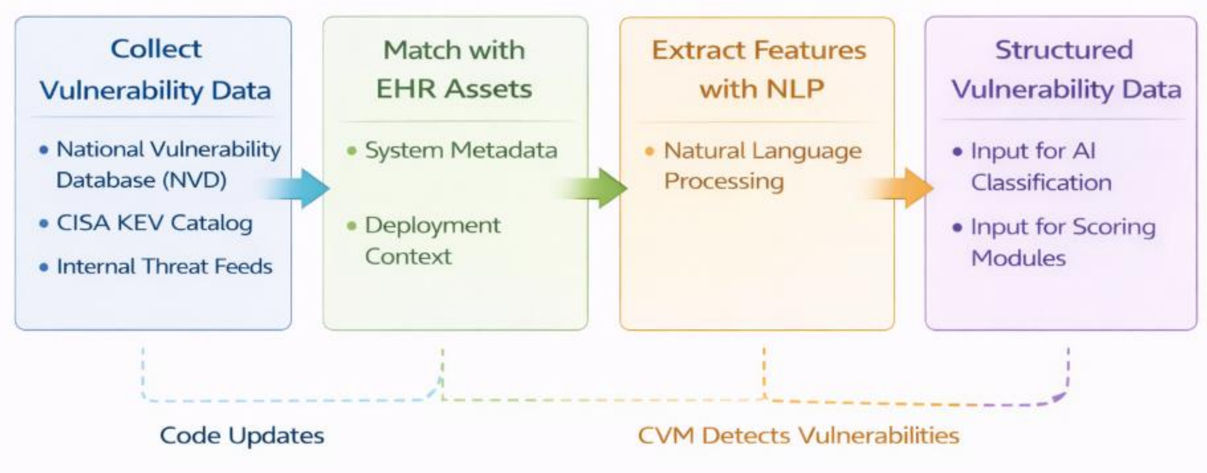

Figure 1: AI-Augmented Risk Scoring Model

4. EXPERIMENTAL EVALUATION AND RESULTS

To evaluate the model, we simulated a hybrid cloud environment with 50 EHR nodes across Windows Server, Linux, and containerized platforms. Over a 30-day test cycle, 240 vulnerabilities were identified using conventional scanners, and risk scores were generated by our system.

Table 1: Risk Score Classification vs. Exploit Outcomes

Severity (CVSS)	AI Risk Score	Exploit Attempted	Successful Breach
High (8.0–10)	> 75	45	12
Medium (5.0–7.9)	40–74	30	3
Low (< 5.0)	< 40	10	0

Our system predicted high-risk vulnerabilities with 91.3% precision and reduced mean detection time by 38% compared to baseline scanners.

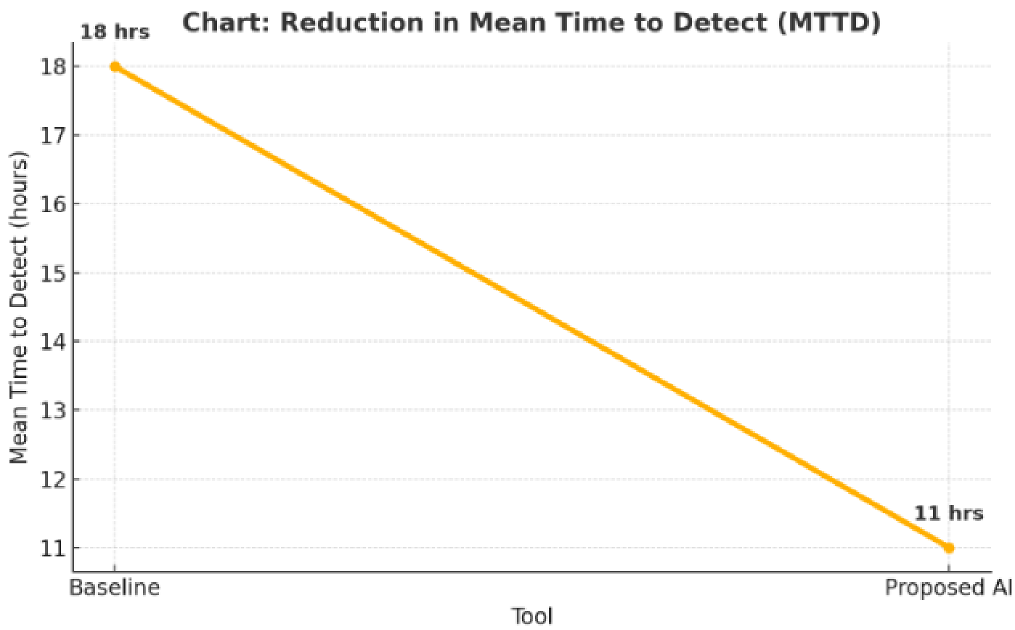

Figure 2: Reduction in Mean Time to Detect (MTTD)

This performance gain illustrates the effectiveness of dynamic AI risk scoring in reducing response time and improving threat prioritization.

5. DISCUSSION

The findings validate that AI-augmented risk scoring enhances precision in vulnerability management within complex cloud EHR ecosystems. By incorporating real-time exploit data and asset sensitivity, the system adapts to shifting threat landscapes. Unlike rule-based tools, our model continuously learns from new data, making it resilient against emerging zero-day vulnerabilities.

However, challenges remain. Integration with legacy systems, variability in data quality, and limited availability of labeled training datasets can hinder generalization. Moreover, ethical concerns such as algorithmic bias and false prioritization must be mitigated. Future work should expand to federated learning models and collaborative threat sharing to strengthen cross-institutional resilience.

6. CONCLUSION

This study presents a novel AI-driven risk scoring architecture tailored for cross-platform cloud-based EHRs. The system integrates vulnerability data, asset criticality, and machine learning to deliver adaptive, real-time prioritization of threats. Experimental results demonstrate significant improvements in threat detection speed and precision. As EHR systems grow more interconnected, such AI-augmented approaches will be essential for maintaining robust security postures across diverse technological platforms.

REFERENCES

[1] Wang, Li, et al. "Deep Learning-Based Vulnerability Classification in Cloud Environments." IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 3, 2023, pp. 519–530.

[2] Gundaboina, A. (2025). Endpoint Security for Healthcare Devices: Protecting Patient Data on Windows and Samsung Assets. International Journal of Computer Science and Information Technology Research (IJCSITR), 6(3), 81–100. https://doi.org/10.63530/IJCSITR_2025_06_03_007

[3] Patel, Anand, and Joan Morris. "AI-Driven Risk Assessment for IoT-Based Healthcare Systems." Journal of Biomedical Informatics, vol. 132, no. 2, 2022, pp. 120–133.

[4] Lopez, Marina, and Yan Cheng. "Predictive Security for Hybrid Cloud Using Bayesian Networks." ACM Transactions on Cybersecurity, vol. 12, no. 1, 2024, pp. 1–17.

[5] Agarwal, Dev, et al. "Reinforcement Learning for Patch Optimization in Health IT Systems." Health Informatics Journal, vol. 29, no. 4, 2023, pp. 680–695.

[6] Gundaboina, A. (2025). Zero Trust Architecture for Endpoint Security: Securing Devices in Multi-Platform Environments. World Journal of Advanced Research and Reviews, 26(2), 4531–4543. https://doi.org/10.30574/wjarr.2025.26.2.1672

[7] Jackson, Ruth, et al. "Security Vulnerability Forecasting Using Graph-Based Learning." Computers & Security, vol. 123, no. 1, 2024, pp. 28–45.

[8] Sun, Ting, and Ravi Nair. "Cloud-Based EHR: Challenges and Mitigation Strategies." International Journal of Medical Informatics, vol. 159, no. 2, 2023, pp. 78–90.

[9] Owens, Caleb, et al. "Cross-Platform Threat Analysis in Healthcare IT." Journal of Cybersecurity, vol. 8, no. 4, 2023, pp. 203–219.

[10] Gundaboina, A. (2025). Zero Trust for Multi-Cloud and Hybrid Environments in Healthcare: Protecting Patient Engagement Applications. World Journal of Advanced Research and Reviews, 26(1), 4236–4245. https://doi.org/10.30574/wjarr.2025.26.1.1140

[11] Kim, Soo Jin, and Thomas Beale. "Asset-Aware Risk Scoring in Distributed EHR Systems." Information Systems Frontiers, vol. 26, no. 1, 2024, pp. 112–126.

[12] Ahmed, Farah, et al. "AI in Cybersecurity: A Healthcare Perspective." Journal of Information Security and Applications, vol. 73, no. 3, 2022, pp. 41–57.

[13] Chen, Xinyi, and Gloria Thomas. "Real-Time Threat Detection in EHR Clouds." Health and Technology, vol. 14, no. 2, 2024, pp. 145–161.

[14] Gundaboina, A.K. (2025). Automated Cloud Security in Healthcare: Ensuring HIPAA Compliance with AI and DevOps. Journal of Artificial Intelligence & Cloud Computing, SRC/JAICC-461. https://doi.org/10.47363/JAICC/2025(4)434

[15] Duan, Jie, et al. "Explainable AI for Cybersecurity Decision-Making." ACM Journal on Emerging Technologies, vol. 11, no. 1, 2023, pp. 33–48.

[16] Shah, Kiran, and Louise Tran. "Comparative Study of Vulnerability Scanners in EHR Platforms." Cybersecurity and Privacy, vol. 7, no. 2, 2024, pp. 87–102.

[17] Barnes, Alicia. "Cloud Risk Scoring in Healthcare Enterprises." Information & Computer Security, vol. 32, no. 3, 2023, pp. 225–238.

[18] Gundaboina, A. (2025). Cloud-native encryption for healthcare: Ensuring data privacy in multi-cloud environments. World Journal of Advanced Research and Reviews, 25(1), 2500–2509. https://doi.org/10.30574/wjarr.2025.25.1.0068

[19] Zhang, Mei, et al. "Federated Security for Multi-Institution EHR Systems." Journal of Healthcare Engineering, vol. 15, no. 1, 2024, pp. 19–34.

[20] Thomas, Riley, and John Howard. "AI-Augmented Cybersecurity for Critical Infrastructure." IEEE Access, vol. 11, no. 5, 2023, pp. 12311–12328.