DOI: doi.org/10.47363/JAICC/ICAIC2025/2025(4)2

Criticality of Cybersecurity for AI in Healthcare's Future

Akhila Harinarayana

Principal Analyst Nelson Hall Bangalore, India

Abstract

The integration of Artificial Intelligence (AI) is revolutionizing healthcare, enhancing diagnostics, personalized treatments, and operational efficiencies. However, this advancement elevates cybersecurity from a technical concern to a critical business imperative. The vast amounts of sensitive patient data and the critical functions entrusted to AI systems expose healthcare organizations to increasing cyber risks, threatening financial stability, operational continuity, and patient trust. Several key trends will shape the future of cybersecurity in this AI-driven landscape. The sophistication of AI-powered cyberattacks will necessitate equally advanced AI-driven defenses. Organizations must invest in security systems that can autonomously learn, adapt, and respond to dynamic threats, outmaneuvering adversaries who leverage AI for more targeted and potent intrusions. The expansion of connected medical devices, or the Internet of Medical Things (IoMT), broadens the attack surface. Future cybersecurity strategies will focus on securing these devices from design through their operational lifecycle, preventing them from becoming vulnerable entry points into broader clinical networks. Ensuring the integrity and trustworthiness of AI systems will be paramount. As AI increasingly informs critical healthcare decisions, protecting these systems from manipulation by malicious actors is vital to guarantee the reliability and safety of AI-driven recommendations and diagnoses.