IJARSCT
ISSN: 2581-9429
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Volume 5, Issue 3, July 2025
Impact Factor: 7.67

AI-Enabled Intrusion Detection Systems for Connected Healthcare Systems: Challenges, Models, and Future Directions

Vijay Kumar Padala[1] and Ayyanki Hema Sundar[2]
Assistant Professor, Computer Science[1]
III BCA[2]
Sir. C. R. Reddy College of Engineering, Eluru

Abstract: *This paper examines the role of AI-enabled Intrusion Detection Systems (IDS) in connected healthcare environments, particularly within the Internet of Medical Things (IoMT). As healthcare systems become more interconnected, they face significant cybersecurity threats such as data breaches, ransom ware, and insider attacks. AI-based IDS offer a promising solution due to their ability to detect anomalies in real time and adapt to evolving threats. However, the implementation of these systems faces challenges, including limited computational resources on medical devices, poor generalizability of machine learning models, lack of explainability, vulnerability to adversarial attacks, and concerns about patient data privacy. The paper reviews various AI approaches like supervised learning, deep learning, reinforcement learning, federated learning, and explainable AI models. It concludes by highlighting the need for lightweight, privacy-aware, and trustworthy IDS frameworks that can function across edge, fog, and cloud layers, while also being tested in real-world clinical environments.*

Keywords*:* Internet of Medical Things

DOI: 10.48175/IJARSCT-28536