IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
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

I. INTRODUCTION

Connected healthcare, often referred to as the Internet of Medical Things (IoMT) or Healthcare 4.0, involves the integration of body sensors, medical devices, communication gateways, cloud/fog computing, and intelligent applications into a unified, multi-layered architecture. This ecosystem enables remote monitoring, predictive diagnostics, and real-time medical intervention. However, the increased interconnectivity exposes the system to critical cybersecurity threats such as man-in-the-middle (MITM) attacks, data tampering, denial-of-service (DoS), ransomware, and malicious manipulation of sensor data (Al-Turjman et al., 2020; Humayed et al., 2017).

To address these security concerns, Artificial Intelligence (AI)-powered Intrusion Detection Systems (IDS) are emerging as vital solutions. Unlike traditional signature-based IDS, which depend on predefined attack patterns, AI-enabled systems can learn from network behavior and detect anomalies, including zero-day and insider threats, with greater precision and speed. These systems enhance scalability, reduce false positives, and provide real-time detection capabilities, making them highly suitable for complex and dynamic healthcare networks (Luo et al., 2021; Rani & Thakur, 2023).

II. CHALLENGES IN AI-ENABLED IDS FOR CONNECTED HEALTHCARE

Implementing AI-based Intrusion Detection Systems (IDS) in connected healthcare environments presents several significant challenges. One of the primary issues is the resource constraint of Internet of Medical Things (IoMT) devices. These devices often lack the processing power, memory, and energy capacity required to support complex AI models, making it difficult to deploy real-time, on-device intrusion detection solutions (Al-Turjman et al., 2020; Sodhro et al., 2021).

Another critical concern is the lack of high-quality, representative datasets. Most publicly available datasets used to train AI-based IDS are outdated, synthetic, or not reflective of real-world healthcare environments. This leads to poor

DOI: 10.48175/IJARSCT-28536

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

generalizability of models and limits their ability to detect sophisticated attacks in diverse settings (Zhou et al., 2022). Additionally, imbalanced datasets can cause AI models to overlook minority class events such as rare but dangerous intrusions, leading to increased false negatives.

Explainability and transparency of AI models also pose major challenges. Deep learning models, although accurate, often operate as "black boxes," providing little insight into their decision-making process. In healthcare, where trust, accountability, and regulatory compliance are critical, such lack of explainability limits the practical deployment of AI-enabled IDS (Arrieta et al., 2020; Roy et al., 2023).

The rise of adversarial attacks and stealthy threats further complicates the deployment of IDS. Attackers can craft inputs that manipulate AI models into misclassifying malicious activities as benign. Moreover, slow-moving, long-dwell attacks that blend with normal traffic patterns are difficult for static AI models to detect, especially in time-sensitive medical environments (Papernot et al., 2018; Hossain et al., 2021).

Finally, privacy and collaboration constraints hinder centralized training of AI models using sensitive patient data. While Federated Learning (FL) has been proposed as a privacy-preserving alternative, it introduces new challenges such as increased communication overhead, model drift, and difficulties in coordinating across heterogeneous devices and institutions (Sheller et al., 2020; Li et al., 2021).

III. CHALLENGES IN AI-ENABLED IDS FOR CONNECTED HEALTHCARE

a. Resource & Deployment Constraints IoMT devices are typically constrained by limited computational power, memory, and energy, which poses a barrier to deploying advanced machine learning (ML) or deep learning (DL) models directly on devices. These limitations restrict real-time, on-device intrusion detection capabilities. While fog or cloud computing can offload processing, it introduces additional latency and network dependency, which are undesirable in time-sensitive healthcare environments (Al-Turjman et al., 2020; Sodhro et al., 2021; Hossain & Muhammad, 2021).

b. Data & Model Issues AI-enabled IDS require large volumes of labeled and representative data. However, available public datasets like KDD'99 or NSL-KDD are outdated, synthetic, or lack healthcare-specific features. These deficiencies lead to overfitting and poor model generalizability across diverse devices, networks, and medical applications. Moreover, class imbalance in datasets (e.g., fewer attack samples) often results in lower detection accuracy for rare but critical threats (Zhou et al., 2022; Diro & Chilamkurti, 2018).

c. Explainability & Trust Most AI models, particularly deep learning-based IDS, are considered "black-box" systems, offering little insight into their decision-making process. This lack of transparency creates significant trust barriers in clinical environments, where accountability and explainability are essential. Although explainable AI (XAI) is growing in general applications, its integration into healthcare-specific IDS remains minimal (Arrieta et al., 2020; Roy et al., 2023).

d. Adversarial & Stealth Attacks AI-based IDS are vulnerable to adversarial attacks where carefully crafted inputs fool the detection models. Attackers can also launch stealthy, long-dwell attacks that evolve slowly, mimicking normal behavior and evading traditional anomaly detection. These advanced threats highlight the need for robust, adaptive, and context-aware IDS in healthcare settings (Papernot et al., 2018; Hossain et al., 2021).

e. Privacy & Collaboration Constraints Training AI models on sensitive patient data raises ethical and legal concerns under regulations like HIPAA and GDPR. Centralized training increases the risk of privacy breaches. Federated Learning (FL) offers a decentralized approach, allowing local model training without data sharing, but it introduces challenges such as communication overhead, data heterogeneity, and model drift (Sheller et al., 2020; Li et al., 2021).

IV. MODELS & APPROACHES

AI-enabled Intrusion Detection Systems (IDS) in connected healthcare systems employ a range of learning techniques and architectural models to address evolving threats.

Supervised ML & Ensemble Methods are widely used for binary and multi-class classification of attack types. Algorithms such as Support Vector Machines (SVM), Decision Trees, Random Forests, and Gradient Boosting achieve

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

high accuracy when trained on well-labeled datasets. Ensemble methods, in particular, improve robustness and reduce false positives by combining predictions from multiple learners (Zhou et al., 2022).

Hybrid Deep Learning (DL) Frameworks, such as those combining Convolutional Neural Networks (CNN) with Long Short-Term Memory (LSTM) or Bidirectional LSTM (BiLSTM), are gaining traction for analyzing spatial-temporal network patterns. CNNs help extract local features from network traffic, while LSTMs capture sequential patterns, enhancing anomaly detection capabilities (Diro & Chilamkurti, 2018).

Deep Reinforcement Learning (DRL) introduces adaptability by enabling IDS to learn optimal detection strategies through interactions with dynamic network environments. This is particularly beneficial for continuously evolving attack patterns and minimizes manual intervention (Nguyen et al., 2019).

Explainable Machine Learning (X-IDS) seeks to improve transparency by integrating interpretability mechanisms into IDS models. Techniques such as SHAP (SHapley Additive exPlanations) or LIME (Local Interpretable Model-agnostic Explanations) are used to explain model decisions, which is essential in clinical settings where accountability is critical (Arrieta et al., 2020).

Federated Learning (FL) is an emerging solution for privacy-preserving intrusion detection, allowing distributed healthcare nodes to train shared models without transferring raw patient data. This approach ensures compliance with privacy regulations such as HIPAA while maintaining model performance across institutions (Sheller et al., 2020).

V. FUTURE DIRECTIONS

To advance AI-enabled intrusion detection in connected healthcare systems, several research directions are crucial. First, lightweight and hybrid edge–fog ML architectures must be developed to meet real-time demands and the resource limitations of IoMT devices. Second, creating temporal and multi-modal datasets will improve model generalization and robustness to context shifts. Third, combining explainability with human-in-the-loop systems can enhance trust, accountability, and decision support in clinical environments. Addressing adversarial robustness through continual learning mechanisms is essential, as static models remain vulnerable to evolving threats. Privacy-preserving and federated learning models should be further optimized to handle heterogeneity and limited communication bandwidth. Additionally, integration with regulatory frameworks (such as HIPAA or GDPR) and development of standardization protocols will ensure ethical and compliant deployment. Finally, real-world deployment and human-centered trials are vital to validate AI-based IDS under practical constraints and user feedback.

Proposed Conceptual Framework (High-Level)

A multi-layered AI-enabled intrusion detection framework for connected healthcare systems can be structured as follows:

- **Device / Edge Layer:** Utilizes lightweight anomaly detectors such as one-class SVM or shallow neural networks to provide real-time detection with minimal latency and low computational overhead, suitable for resource-constrained IoMT devices (Al-Turjman et al., 2020).
- **Fog / Gateway Layer:** Implements hybrid deep learning (DL) and deep reinforcement learning (DRL) models, such as CNN combined with LSTM or DRL-based adaptation, to capture temporal patterns and provide adaptive feedback mechanisms, bridging local detection with cloud intelligence (Diro & Chilamkurti, 2018; Nguyen et al., 2019).
- **Cloud / Server Layer:** Performs global model training and aggregation using federated learning to preserve privacy while benefiting from cross-entity data. Explainability methods are integrated here to ensure transparency and compliance with healthcare regulations (Sheller et al., 2020; Arrieta et al., 2020).
- **Control / Policy Layer:** Applies behavioral trust scoring and policy-aware access control to modulate permissions dynamically based on IDS alerts, providing audit trails for accountability and regulatory compliance (Roy et al., 2023).

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

VI. CONCLUSION

AI-enabled Intrusion Detection Systems (IDS) represent a transformative advancement in securing connected healthcare ecosystems by providing real-time, adaptive, and precise defense against a broad spectrum of cyber threats. These systems leverage the ability of machine learning (ML) and deep learning (DL) techniques to analyze vast amounts of heterogeneous medical and network data, allowing them to detect anomalies, zero-day exploits, and insider threats that traditional signature-based systems often miss. The layered architecture involving edge, fog, and cloud computing facilitates scalable and timely threat detection while balancing resource constraints and latency requirements.

However, the deployment of AI-enabled IDS in healthcare faces substantial challenges. IoMT devices generally operate under strict computational and energy limits, restricting the complexity of on-device AI models and necessitating innovative lightweight or hybrid frameworks. Moreover, the "black-box" nature of many deep learning models raises critical concerns about explainability and trust, which are essential in healthcare environments where decisions can impact patient safety and regulatory compliance. Adversarial threats—such as carefully crafted inputs that evade detection—and stealthy attacks that mimic legitimate behavior further complicate robust detection.

Privacy concerns dominate healthcare data management, with regulations such as HIPAA and GDPR requiring stringent data protection measures. Federated learning and privacy-preserving AI approaches offer promising solutions but introduce challenges in communication overhead and heterogeneous data distribution. Integrating human-in-the-loop approaches can enhance model transparency and trust, allowing clinicians to validate and intervene when necessary.

Looking ahead, the fusion of hybrid DL and deep reinforcement learning (DRL) models, coupled with explainable AI techniques, will drive more intelligent, interpretable, and resilient IDS. Federated learning will enable collaborative model training across distributed healthcare entities without compromising patient privacy. Furthermore, the development of regulatory-compliant frameworks and standardized protocols is critical to facilitate widespread adoption and interoperability.

In summary, AI-enabled IDS have the potential to revolutionize cybersecurity in connected healthcare by offering adaptive, accurate, and privacy-conscious protection. Realizing this potential requires addressing resource limitations, ensuring model transparency, enhancing adversarial robustness, and fostering cross-institutional collaboration—all within an ethically grounded and regulatory-compliant framework.

REFERENCES

[1]. Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., ... & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

[2]. Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, 82, 761–768. https://doi.org/10.1016/j.future.2017.08.043

[3]. Nguyen, N. G., Nguyen, T. T., Nguyen, T. T., Hwang, D., & Nguyen, G. N. (2019). Deep reinforcement learning for cyber security in Internet of Things. IEEE Access, 7, 77807–77826. https://doi.org/10.1109/ACCESS.2019.2921575

[4]. Sheller, M. J., Reina, G. A., Edwards, B., Martin, J., & Bakas, S. (2020). Multi-institutional deep learning modeling without sharing patient data: A federated learning approach for healthcare. Scientific Reports, 10(1), 12598. https://doi.org/10.1038/s41598-020-69250-1

[5]. Zhou, J., Wang, Q., & Xiong, W. (2022). A review on deep learning-based intrusion detection systems in healthcare IoT. IEEE Access, 10, 87021–87039. https://doi.org/10.1109/ACCESS.2022.3198115

[6]. Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2020). An overview of security and privacy in smart healthcare: Challenges, solutions, and recommendations. Computer Networks, 153, 181–200. https://doi.org/10.1016/j.comnet.2019.12.015

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

[7]. Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. IEEE Internet of Things Journal, 4(6), 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172

[8]. Luo, Y., Liu, Y., Hu, W., & Guo, R. (2021). Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities. IEEE Transactions on Industrial Informatics, 17(9), 6534–6544. https://doi.org/10.1109/TII.2020.3046364

[9]. Rani, S., & Thakur, R. S. (2023). A review of artificial intelligence-based intrusion detection systems for Internet of Medical Things. Health and Technology, 13, 1597–1610. https://doi.org/10.1007/s12553-023-00781-3

[10]. Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2020). An overview of security and privacy in smart healthcare: Challenges, solutions, and recommendations. Computer Networks, 153, 181–200. https://doi.org/10.1016/j.comnet.2019.12.015

[11]. Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., ... & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

[12]. Hossain, M. S., Muhammad, G., & Guizani, M. (2021). Explainable AI and mass surveillance system-based healthcare framework to combat COVID-19 like pandemics. IEEE Network, 35(5), 118–124. https://doi.org/10.1109/MNET.011.2000400

[13]. Li, X., Gu, Y., Diao, W., & Tang, M. (2021). Federated learning for privacy-preserving intrusion detection in the Internet of Medical Things. IEEE Journal of Biomedical and Health Informatics, 25(12), 4511–4521. https://doi.org/10.1109/JBHI.2021.3097400

[14]. Papernot, N., McDaniel, P., Goodfellow, I., Jha, S., Celik, Z. B., & Swami, A. (2018). Practical black-box attacks against machine learning. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (pp. 506–519). https://doi.org/10.1145/3052973.3053009

[15]. Roy, P., Saha, R., & Rani, S. (2023). Enhancing trust in AI-driven healthcare systems using explainable models. Health Informatics Journal, 29(1), 14604582231157967. https://doi.org/10.1177/14604582231157967

[16]. Sheller, M. J., Reina, G. A., Edwards, B., Martin, J., & Bakas, S. (2020). Multi-institutional deep learning modeling without sharing patient data: A federated learning approach for healthcare. Scientific Reports, 10(1), 1–12. https://doi.org/10.1038/s41598-020-69250-1

[17]. Sodhro, A. H., Sangaiah, A. K., & Pirbhulal, S. (2021). Green and robust healthcare framework for heartbeat classification using wearable sensors. Computers & Electrical Engineering, 83, 106581. https://doi.org/10.1016/j.compeleceng.2020.106581

[18]. Zhou, J., Wang, Q., & Xiong, W. (2022). A review on deep learning-based intrusion detection systems in healthcare IoT. IEEE Access, 10, 87021–87039. https://doi.org/10.1109/ACCESS.2022.3198115

[19]. Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2020). An overview of security and privacy in smart healthcare: Challenges, solutions, and recommendations. Computer Networks, 153, 181–200. https://doi.org/10.1016/j.comnet.2019.12.015

[20]. Sodhro, A. H., Sangaiah, A. K., & Pirbhulal, S. (2021). Green and robust healthcare framework for heartbeat classification using wearable sensors. Computers & Electrical Engineering, 83, 106581. https://doi.org/10.1016/j.compeleceng.2020.106581

[21]. Hossain, M. S., & Muhammad, G. (2021). Explainable AI and mass surveillance system-based healthcare framework to combat COVID-19-like pandemics. IEEE Network, 35(5), 118–124. https://doi.org/10.1109/MNET.011.2000400

[22]. Zhou, J., Wang, Q., & Xiong, W. (2022). A review on deep learning-based intrusion detection systems in healthcare IoT. IEEE Access, 10, 87021–87039. https://doi.org/10.1109/ACCESS.2022.3198115

[23]. Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, 82, 761–768. https://doi.org/10.1016/j.future.2017.08.043