Are AI Wearables Vulnerable to Hacking? A Deep Dive into Digital Health Security Risks

Rasit Dinc

Rasit Dinc Digital Health & AI Research

Published: January 13, 2023 | AI Diagnostics

DOI: 10.5281/zenodo.17997648

Abstract

Are AI Wearables Vulnerable to Hacking? A Deep Dive into Digital Health Security Risks The convergence of Artificial Intelligence (AI) and wearable tech...

Are AI Wearables Vulnerable to Hacking? A Deep Dive into Digital Health Security Risks

The convergence of Artificial Intelligence (AI) and wearable technology has ushered in a new era of personalized health monitoring. From smartwatches that track heart rhythm to rings that analyze sleep cycles, these devices, often categorized under the Internet of Medical Things (IoMT), promise to revolutionize healthcare by providing continuous, real-time data. However, as these devices become more sophisticated and deeply integrated into our lives, a critical question emerges: **Are AI wearables vulnerable to hacking?** The answer, grounded in academic research and cybersecurity analysis, is a resounding yes, necessitating a deeper understanding of the risks and the necessary countermeasures.

The Foundation of Vulnerability: Traditional IoMT Flaws

The security concerns surrounding AI wearables are twofold, beginning with the fundamental hardware and communication protocols. Many of these devices suffer from vulnerabilities common to the broader IoT landscape. Research has consistently highlighted weaknesses in the **Bluetooth Low Energy (BLE)** protocol, which is the primary method for pairing and transmitting data between the wearable and a user's smartphone [1]. A passive attack on smartwatches, for instance, can expose vulnerabilities during the pairing process, allowing cybercriminals to potentially intercept sensitive health data [1].

Beyond communication, issues such as insecure data storage, a lack of strong encryption, and manufacturer negligence—specifically the failure to provide timely software updates and security patches—create significant entry points for attackers. Compromise of this data not only violates privacy but, in the case of medical-grade wearables, could lead to physical harm if a device's functionality is maliciously altered.

The AI-Specific Threat: Adversarial Attacks and Data Poisoning

The integration of AI introduces a new, more insidious layer of vulnerability that targets the very intelligence of the device. This threat is known as an **adversarial attack**, where subtle, malicious input is introduced to trick the machine learning (ML) model into making an incorrect decision [2].

In the context of AI wearables, an attacker could exploit this by manipulating the sensor data—for example, by generating a specific pattern of noise or a slightly altered signal—that the device's ML algorithm misinterprets. This could lead to a false health reading, such as triggering a non-existent critical heart rate alert or failing to detect a genuine medical emergency like a fall. The goal is not to steal data, but to compromise the **integrity** of the AI's diagnostic or predictive capabilities, which could have life-threatening consequences in a clinical setting.

A related threat is **data poisoning**, where an attacker corrupts the training data used to build the AI model. By injecting malicious or misleading data into the training set, the attacker can degrade the model's accuracy or introduce a hidden backdoor that allows for future manipulation [3].

Securing the Future: AI as Defender and the Path Forward

While AI creates new attack vectors, it is also a crucial component of the solution. The future of IoMT security lies in a multi-layered defense strategy that leverages AI itself. Machine learning algorithms can be deployed to act as sophisticated **Intrusion Detection Systems (IDS)**, analyzing data patterns for anomalies that indicate a cyber threat [4]. By continuously monitoring the device's operational data and communication traffic, AI can identify and flag the subtle manipulations characteristic of adversarial attacks, often faster and more effectively than traditional security measures.

Implementing robust security measures, including end-to-end encryption, secure boot processes, and a commitment from manufacturers to a secure development lifecycle (SDLC), is non-negotiable. For a more in-depth analysis of the ethical and professional implications of these digital health advancements, the resources at [www.rasitdinc.com]() provide expert commentary.

In conclusion, AI wearables are indeed vulnerable to hacking, both through traditional communication flaws and novel AI-specific attacks. However, the risks are not insurmountable. By understanding the dual nature of AI—as both a source of vulnerability and a powerful tool for defense—manufacturers, regulators, and users can collaborate to build a more secure and trustworthy digital health ecosystem. The challenge is to ensure that the pace of security innovation keeps up with the rapid advancement of AI-powered health technology.

References

[1] Silva-Trujillo, A. G., et al. (2023). Cybersecurity Analysis of Wearable Devices: Smartwatches Passive Attack. *Sensors (Basel, Switzerland)*, 23(12): 5438. [https://pmc.ncbi.nlm.nih.gov/articles/PMC10301545/]()

[2] Jha, B. K., et al. (2024). Safeguarding Medical AI: Insights and Addressing Undetectable Adversarial Attacks in the Medical CE Ecosystem. *IEEE Explore*. [https://ieeexplore.ieee.org/document/10636316/]()

[3] Lumenova AI. (2025). Data Poisoning Attacks: How AI Models Can Be Corrupted. [https://www.lumenova.ai/blog/data-poisoning-attacks/]()

[4] Messinis, S., et al. (2024). Enhancing Internet of Medical Things security with artificial intelligence: A comprehensive review. *Computers in Biology and Medicine*, 10845. [https://www.sciencedirect.com/science/article/pii/S0010482524001203]()

Rasit Dinc Digital Health & AI Research

https://rasitdinc.com