Multidisciplinary Journal of Research in Engineering and Technology

ISSN: 2348-6953

Volume 13 Issue 2 (2026) | Pages: 236-242

Security and Privacy Issues in Wearable Devices: An Extensive Review of Threats, Gaps and Future Directions

Jayashree S. Patil[1], Ashutosh M. Gurav[2], Shalaka R. Bajaj[3], Shruti R. Chourasia[4], Sumit B. Khobragade[5], Tanzeem A. Hundekari[6]

123456MCA, MES IMCC, Pune, Maharashtra, India

[1]jsp.imcc@mespune.in, [2]ashutoshgurav71@gmail.com, [3]shalakabajaj2003@gmail.com, [4]shrutichourasia1234@*gmail.com*, [5]sumitbk1010@gmail.com, [6]tanzeem8324@gmail.com

Peer Review Information

***Type**: Article*
***Received:** 17 March 2026*
***Revised:** 04 April 2026*
***Accepted:** 11 May 2026*
***Published:** 01 June 2026*

Abstract

Wearable technology like smartwatches, fitness trackers, and health monitoring devices is becoming a part of everyone's life. Healthcare infrastructure provides convenience and real-time information about personal health. But the one issue that arises is security. The security and privacy of one user's information is at risk. This paper provides a detailed review of wearable devices security, it also concerns serious vulnerabilities at different levels of hardware and software. According to a literature review between 2020 and 2024, major topics like poor authentication, transmission of data without encryption, users were not aware about technology, and lack of adequate legal protection are discussed. The review brings these vulnerabilities that can result in breaches of data transfer, unauthorized activities and misuse of personal data. The results focus on the urgent need for standardization of security measures across different systems, increased regulatory control, and data privacy solutions that majorly concern the user to ensure the security of these wearable devices.[2][10]

Keywords: Wearable Devices, Security, Privacy, Bluetooth Low Energy (BLE), Authentication, IoT

How to Cite This Article

Patil, J. Gurav, A. Bajaj, S. Chourasia, S. Khobragade, S. Hundekari, T. (2026). Security and Privacy Issues in Wearable Devices: An Extensive Review Of Threats, Gaps And Future Directions. *Multidisciplinary Journal of Research in Engineering and Technology*13(2), 236–242.

Introduction

Wearable devices like smartwatches, fitness bands, and health trackers are becoming a regular part of people's daily lives. They offer health reminders and alerts for abnormal vitals. Healthcare professionals are starting to use wearables to keep an eye on patients' vital signs from afar. But at the same time, there are some worries about privacy and security. These devices gather a ton of personal info—where we go, how we're sleeping, our health stats, and sometimes even fingerprints or face scans. Since they're usually linked up to the internet or to our phones, there's a chance hackers could break in and grab that data. As more people start using wearable devices—whether for everyday use or in hospitals—it got us wondering just how secure these gadgets really are. They gather a lot of personal data, and because they're usually linked to our phones or the internet, there could be risks we haven't fully thought about yet.

Compared to phones or computers, wearables don't seem to have as many built-in security features. Most people probably don't think much about whether their smartwatch or fitness band is secure, and honestly, neither did we at least, not until we started looking into it. So, this review is our attempt to understand things better. We're hoping to explore a few main questions:

- What are the common security issues in wearable tech?
- Why might these devices be more at risk than other smart gadgets?
- Why do wearables appear to be more at risk compared to other smart technologies?
- Is it possible to improve wearable security without making the devices too expensive or hard to use?

By addressing these questions, we hope to better understand the current security challenges and offer some suggestions for making wearable devices safer moving forward.

We believe that reviewing the security of wearable devices is important, especially as more people start using them every day. Wearables offer convenience but gather sensitive personal data. That's why it feels necessary to understand how well this information is being protected and whether current systems are doing enough to keep it safe.

Most research overlooks security and privacy. So, reviewing what's been studied so far might help highlight what's missing and where more attention is needed. Hospitals are increasingly using wearables to track patient health, send medication reminders, or alert medical staff if vital signs suddenly change. If these devices are hacked or misused, the consequences could be serious—not just for privacy but for patient safety as well.As these devices continue to grow in popularity and connect to more smart systems through the Internet of Things (IoT), the risks of data breaches could also increase. A review can reveal gaps and guide future security improvements. [11][16]

Methodology:

Inclusion/Exclusion Criteria:

In evaluating the quality and appropriateness of research to be considered for inclusion, *the following criteria were used:*

- Temporal Scope: 2020-2024 articles were utilized to provide information regarding the prevalent trends and issues of wearable technology.
- Only English language journals were utilized.
- Types of Sources: Peer-reviewed journals, conference papers, and original white papers or technical reports were used to carry out the research.
- Subject Matter Significance: The investigation must focus on security and privacy issues associated with wearable technology, including but not limited to smartwatches, fitness trackers, smart glasses, and health monitoring systems.

The exclusion criteria were:

- Wearable technology, or the design of devices, has been the focus of research while ignoring security and privacy concerns.
- Literature on the broad subject matter of Internet of Things (IoT) security, but without a specific reference to wearable technology.
- Redundant research work, non-academic outputs, opinion pieces, and commentaries.
- These standards assisted in condensing a broad and cross-disciplinary subject matter into the most relevant and significant body of literature.

Databases searched:

The research methodology pursued within this study was the development of a comprehensive database with peer-reviewed articles relevant to security issues and privacy factors regarding wearable technology. Electronic databases used are:

- IEEE Xplore
- ACM Digital Library
- ScienceDirect
- SpringerLink

- PubMed
- Google Scholar

Search Query & Keywords:

Search queries were created using a mix of Boolean operators and search terms. Below is the list of keywords and the search strings utilized:

Basic Keywords:

- "Wearable devices"
- "Smart wearables"
- "Fitness trackers"
- "Smartwatches"
- "health monitoring equipment"

Security/Privacy Keywords:

- "Security threats"
- "Cybersecurity"
- "data breaches"
- "Privacy issues" "Data protection"
- "Authentication" Encryption

Search Queries:

- (Wearable technology, smart wearables, or health monitoring devices) AND (security vulnerabilities, data breaches, or information security) "(Smartwatches or health monitoring devices) AND (privacy issues, data privacy, or data protection)" "Wearable authentication, encryption, or access control technology."
- Truncation and wildcards were used wherever feasible to accommodate spelling differences in the terms (e.g., secur*, privac*, wearabl*). Search filters for the databases were used in publication year, document type, and language fields. [5][7]

Findings and Thematic Analysis

The reviewed literature reveals a recurring pattern of security and privacy issues affecting modern wearable technologies. These vulnerabilities span across hardware-level weaknesses, software flaws, user behavior, and gaps in legal protections. This section outlines the key findings and discusses four major themes that emerged during the analysis. [2][9]

Key Findings

Across the studies, five prominent categories of vulnerabilities were consistently observed:

- *Unencrypted Data Transmission:*
  Many wearable devices transmit personal and health-related information over unsecured Bluetooth Low Energy (BLE) channels. This exposes users to the risk of eavesdropping and unauthorized access to sensitive data.
- *Weak or Absent Authentication:*
  A significant number of devices use outdated pairing models such as “Just Works” or rely on simplistic PIN codes. These methods fail to offer adequate protection against spoofing and brute-force attacks.
- *Lack of Address Randomization:*
  BLE-enabled devices frequently broadcast static MAC addresses, allowing persistent tracking of users over time and across different locations.
- *Software-Level Vulnerabilities:*
  Companion applications are often poorly secured, with excessive permissions and a lack of regular security testing, increasing the risk of data breaches.
- *Insufficient Legal Protections:*
  Existing regulations, such as HIPAA and GDPR, offer limited coverage for data generated by consumer wearables, leaving users' health information exposed in non-clinical contexts. [7][17]

Theme 1: Device-Level Security Deficiencies

One of the most consistent findings across the literature is the lack of built-in security in wearable devices, particularly at the hardware and BLE protocol levels.

Many devices continue to use older versions of BLE (4.0 and 4.1), which lack features like encrypted communication and address randomization. Devices such as the *Polar H7* heart rate monitor and the *Bluebyte Bluetooth Keyboard* have been shown to transmit data in plain text, making it easy for attackers to intercept sensitive information.

Authentication mechanisms are also a concern. Several wearables rely on the “Just

Table 1: Device Security Overview

Device	BLE Version	Encryption	MAC Randomization	Key Vulnerability
Fitbit Charge	4.1	Yes	No	Brute-force attack via PIN
Polar H7	4.0	No	No	Heart rate data leakage
Bluebyte Keyboard	4.0	No	No	Plaintext keystroke logging

Works" pairing model, which offers no identity verification, making devices vulnerable to man-in-the-middle (MITM) and spoofing attacks. Other devices, like the *Fitbit Charge*, use weak PIN-based protection—typically 4 digits—leaving them open to brute-force attempts.

These weaknesses have led to real-world cases of data exposure. For example, both Fitbit and Polar devices were found to leak health data through BLE advertising packets. The Bluebyte keyboard transmitted keystrokes in unencrypted form, creating serious risks when users typed passwords or personal information. [14][15]

Theme 2: Privacy Risks and User Awareness Gaps

Despite growing public concern about data privacy, many users of wearable technology remain unaware of how their data is collected, stored, and shared. This disconnect—commonly referred to as the "privacy paradox"—was a recurring observation across the literature.

In one study, 64% of participants expressed concerns about unauthorized access to their health data. However, many of these users still prioritized convenience and usability over robust privacy settings. This tendency to trade privacy for ease-of-use has significant implications in the context of wearables, which continuously collect sensitive personal data.

Transparency is another critical issue. Privacy policies for wearable devices are often lengthy, complex, and filled with technical jargon, making them inaccessible to the average user. Moreover, devices rarely provide clear notifications about how data is stored or whether it is shared with third-party services or advertisers.

Unauthorized data use is also widespread. Many wearables collect GPS, heart rate, and activity data, which is later repurposed for marketing and analytics—often without the user's explicit consent. The acquisition of Fitbit by Google, for example, raised concerns about how such health data could be monetized.[20]

Summary of Key Issues:

- Users are frequently unaware of:
    - What types of data are being collected.
    - Where and how the data is stored.
    - The extent of legal protection applicable to their data. [8][10]

Theme 3: Infrastructure and Communication Vulnerabilities

Wearable devices depend heavily on wireless communication protocols, particularly BLE, which presents several vulnerabilities in both the physical and application layers.

Research has shown that smartwatches and smart rings are susceptible to a range of BLE-based attacks. These include Adversary-in-the-Middle (AITM) attacks, where a malicious party intercepts communication between devices; key negotiation downgrades, which force devices to use weaker encryption settings; and BLE presence detection, which enables third-party tracking based on device signal patterns.

Companion applications are also a major area of concern. In one analysis, 70% of BLE-enabled health apps were found to be vulnerable to co-located attacks. These attacks exploit weak storage of long-term keys (LTKs), allowing attackers to impersonate or control devices remotely.

Transmission security is another gap. BLE traffic is often not encrypted end-to-end, and mutual authentication is rarely implemented. This increases the risk of data tampering or unauthorized device access.

Recommended Countermeasures:

- Adoption of NIST SP 800-121 guidelines to strengthen BLE communication security.
- Implementation of DevSecOps practices in the development lifecycle to ensure early and continuous integration of security measures. [7][13]

Theme 4: Regulatory and Legal Oversight Limitations

One of the most significant concerns raised in the literature is the inadequacy of current legal frameworks in addressing the privacy and security challenges of wearable technologies.

In the United States, HIPAA (Health Insurance Portability and Accountability Act) only applies to data handled by specific healthcare providers and does not extend to data collected by consumer fitness devices. In the European Union, the General Data Protection Regulation (GDPR) offers broader coverage, but still includes exceptions—such as for anonymized or employer-monitored data—that weaken its applicability to wearables.

Moreover, there are no mandatory international standards that require manufacturers to follow strict security guidelines for wearable technology. Regulatory frameworks from organizations such as the FDA or ACSC often issue voluntary guidance, which many low-risk devices are not obligated to follow.

To address these challenges, some researchers have proposed introducing a Bluetooth Security Facts Label, modeled after nutrition or energy labels. This would allow consumers to easily compare security features when selecting wearable products. Others argue for expanding HIPAA and GDPR to explicitly include biometric and wearable-generated data under protected health information.

Key Legal Risks:

- Employers could exploit health data for performance monitoring or discrimination.
- Stolen wearable data could be used in identity theft, insurance fraud, or social profiling. [1][18]

Summary Table 2: Cross-Paper Themes and Contributions [13][16]

Theme	Supporting Studies	Type of Risk
Device-Level Security Deficiencies	Nebraska, Smart Rings, Model.docx	Technical
Privacy Risks and User Awareness	Model.docx, IJNSA 2016, Smart Rings	Behavioral / Social
Infrastructure and Communication Risks	Smart Rings, Nebraska, Model.docx	Network / Protocol-level
Legal and Regulatory Oversight Gaps	Model.docx, Smart Rings, IJNSA 2016	Policy / Legal

Discussion

Gaps in Literature :

While the security and privacy challenges of wearable devices have been widely studied, several critical gaps still remain that limit the depth and applicability of existing research.

Most existing studies identify known vulnerabilities such as Bluetooth Low Energy (BLE) attacks, weak authentication, and unencrypted data transmission — but few demonstrate real-world exploitation scenarios or measure the actual impact on end-users in practical settings. There is also a notable absence of longitudinal studies that track how the threat landscape evolves as wearable technology advances over time.

Furthermore, the majority of research remains narrowly focused on smartwatches and fitness trackers, while other growing wearable categories such as smart rings, implantable medical devices, smart clothing, and AR/VR headsets remain significantly understudied from a security perspective.

Although machine learning-based anomaly detection and privacy-preserving protocols are emerging as promising solutions, their real-world deployment and scalability in resource-constrained wearable environments have not been adequately validated. Most proposed solutions are tested only in controlled or simulated environments, leaving a gap between theoretical models and practical implementation.

On the regulatory front, while frameworks like GDPR and HIPAA are frequently cited, there is limited research analyzing how effectively these regulations are enforced in practice for consumer wearables, and whether manufacturers are actually complying with security-by-design principles.

Finally, user-centric research remains insufficient. Few studies examine how users perceive, respond to, or adapt their behavior based on security risks — and how UI/UX design changes could nudge users toward better security practices without sacrificing usability.[4][19]

Conclusion

Research emphasizes the important need to increase security and privacy in weekly technologies, especially smart watches and Bluetooth Low Energy (became) devices. Current studies suggest that despite BLA's underlying safety facilities, many wearables are unable to implement them-assess users to be unsure of tracking, data violations and unauthorized access. While smart watches and other wear and tear cause convenience and data communication in real time, they also create significant risks due to their ability to collect sensitive personal information, including health information, location and accounting.

The conclusions have insufficient integration of safety measures in a recurring subject design phase. Safety often occurs later, causing expensive weaknesses. In addition, there is a lack of standardized privacy law, and there is less in defining security for data collected to use existing laws such as GDPR and HIPAA. Limited awareness between users and inadequate manufacturers is leading these risks forward.

Recommendations include the implementation of compulsory security policy to use equipment, cooperate with authorities and industry organs and increase consumers' awareness through equipment such as Bluetooth Security Facts Label (BSFL). When it continued to develop, especially with the release of Bluetooth 6.0, and with Quantum Computing Progress, further research was needed to address new dangers and develop cryptographic solutions by quantity. Ultimately, ensuring the safety of portable technologies requires a coordinated effort to promote a safe and privacy ecosystem among manufacturers, decision makers and users. [7][18]

References

1. Academia.edu. (n.d.). *Wearable devices in healthcare: Privacy and information security issues*. Retrieved from https://academia.edu
2. Academia.edu. (n.d.). *Wearable technology devices security and privacy vulnerability analysis*. Retrieved from https://academia.edu
3. Academia.edu. (n.d.). *Towards evaluating the security of wearable devices in the Internet of Medical Things*. Retrieved from https://academia.edu
4. Academia.edu. (n.d.). *Assessment of security vulnerabilities in wearable devices*. Retrieved from https://academia.edu
5. Semantic Scholar. (n.d.). *The effectiveness of IoT-based wearable devices and potential cybersecurity risks: A systematic literature review from the last decade*. Retrieved from https://www.semanticscholar.org
6. Semantic Scholar. (n.d.). *Cybersecurity analysis of wearable devices: Smartwatches passive attack*. Retrieved from https://www.semanticscholar.org
7. Semantic Scholar. (n.d.). *Security and privacy threats for Bluetooth Low Energy in IoT and wearable devices: A comprehensive survey*. Retrieved from https://www.semanticscholar.org
8. DOAJ. (n.d.). *Determinants of user acceptance of wearable IoT devices*. Retrieved from https://doaj.org
9. PhilPapers. (n.d.). *Cyber security risks in wearable devices*. Retrieved from https://philpapers.org
10. PhilPapers. (n.d.). *Privacy and security of wearable devices*. Retrieved from https://philpapers.org
11. PhilPapers. (n.d.). *Challenges and recommendations for wearable devices in digital health: Data quality, interoperability, health equity, fairness*. Retrieved from https://philpapers.org
12. PhilPapers. (n.d.). *Wearable technologies for healthy ageing: Prospects, challenges, and ethical considerations*. Retrieved from https://philpapers.org
13. BASE. (n.d.). *Smart rings, smarter threats*. Retrieved from https://www.base-search.net
14. BASE. (n.d.). *On the security of Bluetooth Low Energy in two consumer wearable heart rate monitors/sensing devices*. Retrieved from https://www.base-search.net
15. BASE. (n.d.). *Cybersecurity analysis of wearable devices: Smartwatches passive attack*. Retrieved from https://www.base-search.net

16. BASE. (n.d.). *Cyber security of smart watches: A review of the vulnerabilities with recommendations presented to protect the wearables*. Retrieved from https://www.base-search.net
17. ResearchGate. (n.d.). *Vulnerability analysis and exploitation attacks on smart wearable devices*. Retrieved from https://www.researchgate.net
18. CORE. (n.d.). *From Fitbits to pacemakers: Protecting consumer privacy and security in the healthtech age*. Retrieved from https://core.ac.uk
19. CORE. (n.d.). *Security and privacy of wearable Internet of Medical Things: Stakeholders perspective*. Retrieved from https://core.ac.uk
20. ResearchGate. (2017). Real-time critical patient eHealth monitoring system using smart wearables. Retrieved from https://www.researchgate.net