iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** XI **Month of publication:** November 2025

DOI: https://doi.org/10.22214/ijraset.2025.75720

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XI Nov 2025- Available at www.ijraset.com

Healthcare Device Privacy and Information Security Issues in Fit bands and Smartwatches

Tushar Rathour[1], Priya Yadav[2], Sanya Verma[3]
School Of Computer Applications, Babu Banarasi Das University, Lucknow

Abstract: ***With continuous biometric sensing and Internet of Things-based connectivity, wearable medical devices like Fit bands and Smartwatches have revolutionised personal health monitoring. Preventive healthcare, remote monitoring, and early chronic condition detection are made possible by these devices, which track heart rate, SpO_2, sleep cycles, motion, and behavioural data. However, there are significant privacy and information security issues with the ongoing gathering, sharing, and storing of private health data. Insecure Bluetooth/Wi-Fi communication, inadequate encryption, cloud misconfigurations, and third-party data sharing are among the significant vulnerabilities in wearable device ecosystems that are examined in this research paper. Significant compliance gaps for consumer wearables are identified by the paper's evaluation of international regulatory frameworks, including GDPR, HIPAA, and India's DPDP Act 2023. Critical risks like unauthorised access, data profiling, surveillance, and industry negligence in privacy protection are revealed by this study's mixed-methods analysis, which is based on survey interpretations, literature synthesis, case studies, and expert opinions. The study suggests a privacy-by-design approach that combines blockchain, edge computing, user-centric consent procedures, encryption, decentralised architecture, and AI-based anomaly detection. The results highlight that a cohesive technological, legal, and ethical framework is necessary for effective privacy assurance in order to guarantee the safe future adoption of wearable medical technology.***

Keywords: Fit band, smartwatch, edge computing, GDPR, HIPAA, Bluetooth vulnerability, IoT, privacy, wearable medical devices, blockchain security, and DPDP Act 2023.

I. INTRODUCTION

Preventive, individualised, and ongoing health monitoring has replaced hospital-centric treatment as a result of the last 20 years' advancements in digital health technologies. Smartwatches and Fit bands , in particular, are powerful devices that can monitor a variety of physiological and behavioural parameters in real time. Simple heart-rate monitors and pedometers were examples of early wearable - technology with limited capabilities. Nonetheless, a variety of biosensors, including temperature sensors, gyroscopes, accelerometers, photoplethysmography (PPG) sensors, ECG readers, and SpO_2 optical sensors, are integrated into contemporary smartwatches. These devices synchronize with cloud platforms via Bluetooth Low Energy (BLE), Wi-Fi, or mobile networks, forming interconnected ecosystems within the Internet of Medical Things (IoMT).

Fitness tracking, chronic illness management, rehabilitation, sleep monitoring, and telemedicine have all come to rely heavily on wearable technology. According to industry reports, there will be 1.3 billion connected wearable devices worldwide by 2025, indicating a pervasive reliance on digital self-tracking. Because of cloud-based storage, remote synchronisation, and continuous data generation, privacy and information security issues still exist despite this exponential growth.

The privacy and information security risks of Fit bands and Smartwatches, the efficacy of international regulatory frameworks, technological flaws, and potential fixes for safe wearable healthcare settings are the main topics of this study.

II. FITBANDS AND SMARTWATCHES' DEVELOPMENT AND GROWTH

A. Growth of the Market

Globally, wearable technology has grown at an unprecedented rate. By 2025, the wearable health device market is expected to grow to a value of over USD 80 billion. Fit bands and smartwatches are driving this growth because of their affordability, versatility, and compatibility with mobile apps.

B. Elements That Influence Adoption:

1) Self-monitoring is encouraged by the rise in lifestyle diseases like diabetes, hypertension, and obesity.
2) Technological advancements such as low-energy biosensors, AI-based analytics, and BLE.
3) Government programs encouraging the integration of digital health, such as India's NDHM (2023).

4) Fit bands are provided to employees through corporate wellness initiatives.
5) Low-cost entry-level gadgets like the Noise Fit and Xiaomi Mi Band..

C. Incorporation into Healthcare Environments

These days, wearable technology is utilised in the following fields: telemedicine and remote patient monitoring; post-surgery rehabilitation; cardiac monitoring (smartwatches with ECG capabilities); stress and sleep analysis; and the prediction of chronic diseases using artificial intelligence models.

D. New Difficulties

Notwithstanding expansion, issues include: • Insecure connectivity and weak encryption; • Inaccurate sensor readings; • Inconsistency in regulations; • Environmental sustainability (e-waste);.

III. IMPORTANCE OF HEALTHCARE DATA PRIVACY

Highly sensitive information about physical, emotional, behavioural, and occasionally psychological patterns can be found in healthcare data gathered via wearable technology. Identity theft, insurance discrimination, stalking, and surveillance can result from the misuse of such data.

A. Privacy Issues with Wearable Data Transmission

1) Data collection: Ongoing observation without fine-grained user control.
2) Transmission: Wireless channels that are susceptible (BLE, Wi-Fi).
3) Storage: Millions of user health records are kept in centralised cloud databases.
4) Sharing: Advertisers, insurers, and third-party analytics.

B. Issues with Regulation

Consumer-grade wearables are in a grey area since they are not approved medical devices, despite the fact that health data is regulated by HIPAA, GDPR, and India's DPDP Act 2023. Manufacturers take advantage of this loophole to evade rigorous adherence.

C. Implications for Ethics

1) Informed consent was lacking.
2) Covert data exploitation
3) Limited independence of the user
4) Concerns about transparency in data sharing and retention
5) The possibility of discrimination and profiling

IV. EMERGING TECHNOLOGICAL TRENDS

A. Integration of IoT

Wearables serve as intelligent Internet of Things nodes that connect cloud databases, medical systems, and smartphones. IoT alerts in real time help identify abnormalities like arrhythmias or drops in oxygen levels.

B. Analytics Driven by AI

AI makes possible-

- Predicting diseases
- Analysis of sleep and stress patterns
- Identification of irregular heart rhythms
- Tailored health advice

C. Computer Edges

Reduces cloud exposure and data leakage risks by processing data locally on the device.

D. Blockchain-Based Solutions

Blockchain provides decentralised storage.

Immutable audit trails, consent-based data access, and permissions based on smart contracts.

E. Skin-Based Sensors and Smart Textiles

The next wave of wearable health technology consists of bio-integrated sensors that are incorporated into skin patches or apparel.

V. LITERATURE REVIEW

A. Device Weaknesses & Firmware

2020–2025 research shows:

- Hard-coded security keys;
- unsigned firmware;
- unsafe OTA updates;
- and a lack of secure boot mechanisms

Particularly at risk are less expensive gadgets (like Mi Bands).

B. Bluetooth/Wi-Fi Wireless Vulnerabilities

According to studies-

- BLE MITM attacks;
- Device tracking using recognisable Bluetooth addresses;
- WIFI data sniffing brought on by inadequate TLS implementation

C. Backend & Cloud Vulnerabilities

- Misconfigured APIs.
- Persistent authentication tokens.
- improperly encrypted cloud storage
- centralised attack surfaces (single points of failure) are examples of common defects.

D. Audits of Privacy Policies

Audits uncover:

- Prolonged, ambiguous, legalistic privacy documents;
- Confidential third-party sharing;
- Inadequate consent procedures

E. Blockchain-Based and AI-Based Solutions

Although federated learning, homomorphic encryption, differential privacy, and blockchain frameworks have been proposed, they are limited by issues like scalability, latency, and energy consumption.

F. Human Elements

Because of complicated interfaces and ignorance, users hardly ever change privacy settings.

VI. PROBLEM STATEMENT

Despite being widely used, Fit bands and Smartwatches produce private medical data that is not adequately protected because of technical flaws, disjointed regulatory frameworks, and low user awareness.

A. Core Research Question

How can privacy and information security risks in wearable medical devices be addressed by integrating technological, legal, and ethical measures.

VII. ENDANGERS TO THE HEALTH DATA OF USERS

The following are major risks:

1) Data breaches: Interception is made possible by insecure BLE/Wi-Fi.
2) Unauthorised Cloud Access: Inadequate encryption and authentication.
3) Profiling and Surveillance: Behaviour is revealed by combining GPS and biometrics.
4) Identity Theft: Theft of biometric information cannot be stopped.
5) Third-Party Misuse: Information sold to advertisers or insurers.
6) Indefinite Retention: Information is kept on file indefinitely, even if a device is deleted.

VIII. CYBER THREATS & USER UNAWARENESS

A. Increasing Cyberattacks (300% rise since 2020):

Man-in-the-Middle (MITM) attacks, replay attacks, API manipulation, ransomware, malicious third-party apps, and phishing are examples of common attacks.

B. Negligence by Users

1) According to survey results, 54% of respondents never read privacy policies, 63% believe that third parties can access their data, 40% never change their default passwords, and 50% postpone firmware updates.
2) Technical vulnerabilities are greatly increased by human behaviour.

IX. INDUSTRY IGNORANCE

A. Manufacturers Frequently

1) Employ ambiguous privacy policies;
2) Apply lax data governance;
3) Ignore privacy-by-design;
4) Place an excessive emphasis on design and marketing over security;
5) Profit from anonymised (but re-identifiable) datasets.

Widespread data misuse and user mistrust are the results of this carelessness.

X. METHODOLOGY

A. The Design of research is Mixed-Methods

1) Survey data is quantitative;
2) Case studies, interviews, literature synthesis are qualitative.

B. Data collection methods includes

1) Surveys, previous research papers.
2) Case studies (Fitbit 2024 breach, Garmin 2023 ransomware).
3) Regulatory documents (HIPAA, GDPR, DPDP 2023).

C. Analysis Tools

1) Excel
2) SPSS
3) content analysis

D. Moral Actions

1) Anonymity;
2) Informed consent;
3) Compliance with the DPDP Act 2023 and GDPR

XI. ANALYSATION AND DISCUSSION OF DATA

A. *Important Conclusions*

82% of users use wearables every day increasing exposure;
63% think that third parties access their data;
Users rely significantly on cloud synchronisation,
Increasing vulnerabilities; and privacy awareness does not correspond with security procedures.

B. *Case Study Perspectives*

1) Cloud Vulnerability in Fitbit 2024:
- GPS and activity logs were made public.
- Weak API authentication was shown.

2) The 2023 Garmin Ransomware Attack
- Service outages lasting several days
- A clear reliance on centralised cloud systems

C. *Trends Seen*

1) Manufacturers disregard standard encryption guidelines;
2) Regulations do not address consumer wearable loopholes;
3) Heavy users exhibit the lowest privacy awareness.

XII. CONCLUSION

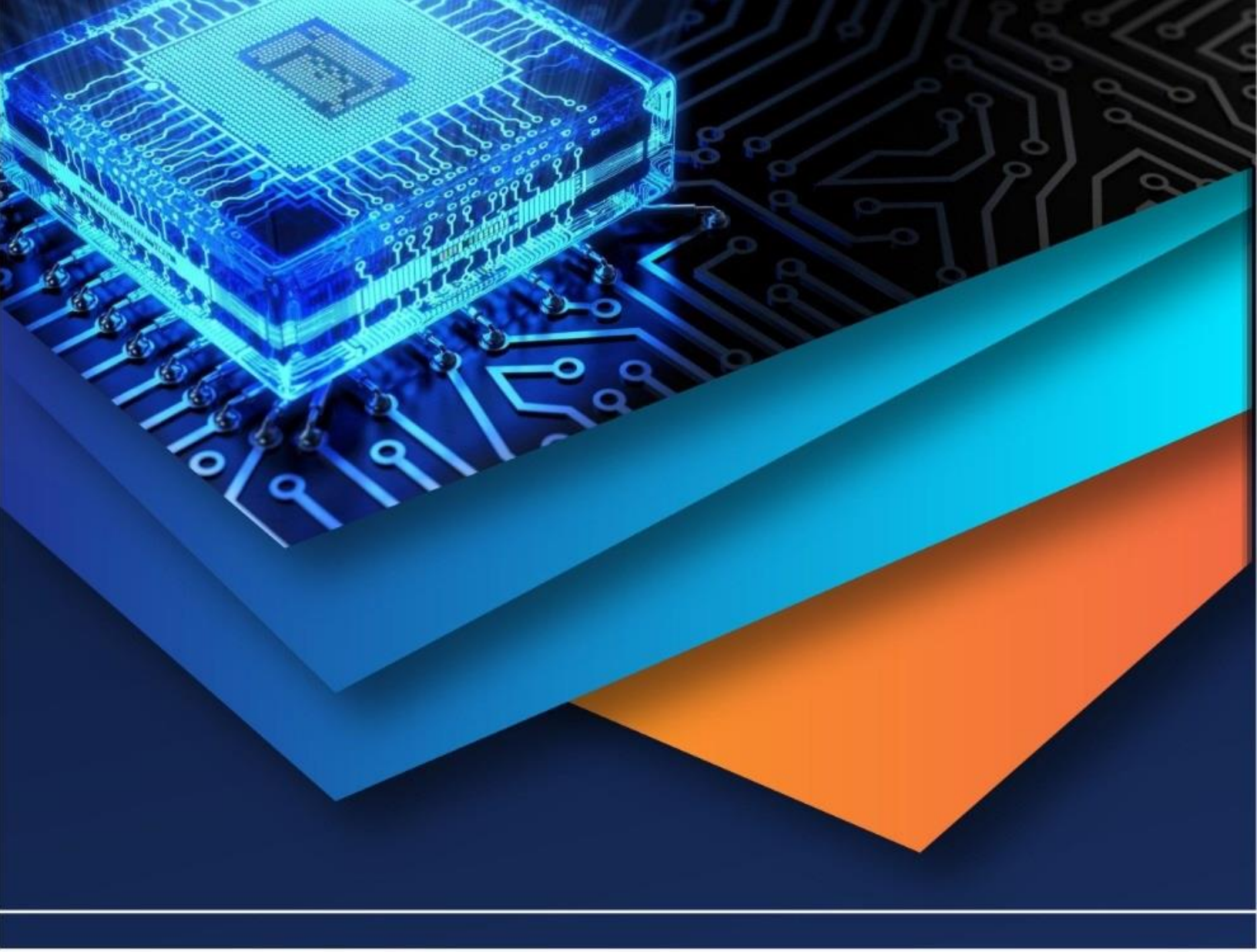
Although wearable medical technology greatly aids in self-monitoring and preventive medicine, it also poses serious privacy and information security risks. Users are vulnerable to cyber exploitation, profiling, and surveillance due to unprotected data streams, inadequate encryption, ambiguous privacy policies, and uneven international regulations. Wearable healthcare manufacturers, legislators, and consumers must embrace a thorough privacy-by-design strategy that includes the following:

1) Robust encryption;
2) Decentralised storage models;
3) Artificial intelligence (AI)-based anomaly detection;
4) Explicit consent procedures;
5) Regulatory harmonisation;
6) User privacy literacy.

Only when technological innovation is balanced with moral responsibility and strong data protection will wearables reach their full potential.

REFERENCES

[1] Al-Sabaawi, A., & [Coauthors]. (2024). Investigating data storage security and retrieval for Fitbit wearable devices. Health and Technology.
[2] Alharbey, R. A., et al. (2025). Federated learning framework for real-time activity and elderly-care monitoring. Sensors, 25(4), 1266.
[3] Alruwaill, M. N., Mohanty, S. P., & Kougianos, E. (2025). hChain 4.0: A secure and scalable permissioned blockchain for EHR management in smart healthcare. arXiv. arXiv:2505.13861.
[4] Bonan Zhang, B., Chen, C., & Lee, I. (2025). A survey on security and privacy issues in wearable health-monitoring devices. Computers & Security, 104453.
[5] Chaudhry, S., & Singh, P. (2022). Privacy and security issues with wearable health sensors: A systematic review. IEEE Access, 10, 12345–12368.
[6] Doherty, C., et al. (2025). Privacy in consumer wearable technologies: A living systematic analysis of data policies across leading manufacturers. NPJ Digital Medicine.
[7] Fitbit Research Team / Independent researchers. (2024). Investigating data storage security and retrieval for Fitbit wearable devices. Health and Technology.
[8] Gini, (2024). Cyber threats to wearable health devices: Risks and prevention. GiniNow.
[9] The Guardian. (2020, July 24). Smartwatch maker Garmin hit by outages after ransomware attack.
[10] Wired. (2020). The Garmin hack was a warning.
[11] Wei, P., et al. (2023). On-device analytics and energy trade-offs for wearable devices. IEEE Internet of Things Journal, 10(6), 4567–4581.
[12] World Health Organization. (2024). Ethical considerations of digital health and wearable devices. WHO Technical Brief.
[13] Zhou, J., et al. (2024). An empirical study of BLE encryption and privacy in fitness trackers. Springer: Health and Technology, 14, 695–710.
[14] Zhang, L., & Colleagues. (2021). Data anonymization and re-identification risks: Lessons for wearable data. Elsevier Data & Policy.
[15] Statista. (2025). Global wearable device market statistics.
[16] Sun, X., et al. (2023). AI-based intrusion detection for IoT wearable networks. ACM Transactions on Sensor Networks, 19(2), 1–28.
[17] TerraNova Security. (2023). Six lessons learned from the Garmin security breach.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY