SPECTRUM OF ENGINEERING SCIENCES
ISSN (E) 3007-3138 (P) 3007-312X VOLUME 4, ISSUE 3, 2026

SECURITY CHALLENGES AND DATA INTEGRITY GAPS IN BLUETOOTH-ENABLED WEARABLE HEALTH DEVICES: A FOCUSED REVIEW

Muhammad Ali Bohyo[*1], Mariya Qazi[2], Sarmad Shams[3], Fahad Shamim[4], Sehreen Moorat[5]

[*1,2,3,4,5]*Liaquat University of Medical and Health Sciences, Jamshoro*

[*1]ali@lumhs.edu.pk

DOI: https://doi.org/10.5281/zenodo.21356009

Keywords
smartwatches, wearable healt monitoring, Bluetooth security, data integrity, pairing vulnerability passive attacks, MITM, secur connections.

Article History
Received: 01 February 2026
Accepted: 17 March 2026
Published: 31 March 2026

Corresponding Author: *
Muhammad Ali Bohyo

Abstract

The advent of smartwatches with health-tracking features has changed the wa people take care of their wellness to a great extent. What were initially basic step counting devices have now developed into devices with sensor capabilities o advanced biometrics, such as electrocardiography (ECG), blood oxygen saturation (SpO2) and sleep tracking. The present review is based on a critical evaluation o six popular smartwatches introduced between 2015 (e.g., Apple Watch Series 1 and 2024 (e.g., Samsung Galaxy Watch 7) in terms of their technologica development, health features, and the security characteristics.Chronologically, th early-generation gadgets (2015-2018), like the Apple Watch Series 3 and Fitbi Versa, focused mostly on the simple fitness tracking, with the heart-rate monitorin and GPS features. These models were mostly based on Bluetooth 4.0/4.2 connectivity, and they had a low battery life of about 18-24 hours. The evolution of devices in the mid-era (2019-2021) with the introduction of the Apple Watch Series 6 and Garmin Venu 2 offered a step in the right direction of a more holisti approach to health monitoring with the inclusion of SpO2 and sleep staging plu fall detection. Nevertheless, the use of Bluetooth communication is a major securit issue despite such improvements. As a result of pairing mechanisms, especially th continued use of Just Works mode, devices are susceptible to man-in-the-middl (MITM) attacks prevailing in several generations of devices. Though mid generation watches presented elliptic-curve Diffie-Hellman (ECDH) key exchange forward secrecy constraints still existed. In the modern models, improved privac characteristics in Bluetooth 5.4 and LE Secure Connections 2 are already used nevertheless, our passive security study indicates persisting vulnerabilities, such a a low PIN entropy, and the unencrypted metadata. It is noteworthy that none o the proposed devices include end-to-end verification of the data integrity, leavin confidential health information vulnerable to manipulation.To sum up, th development of smartwatch hardware and health-monitoring features has increase significantly, yet the security mechanisms did not keep up. This loophole highlight the necessity of a standard approach to data-integrity checks which are wearabl health device specific. Implementing more rigorous Bluetooth pairing criteria lik the mandatory numeric comparison and the use of certificates to pin should b regarded as necessary. It is important to tackle these issues to support the safe usag of wearables in telemedicine and individual healthcare uses.

1. INTRODUCTION

Wearable health devices, particularly smartwatches, have rapidly transitioned from lifestyle accessories to systems capable of continuous physiological monitoring. Modern devices integrate sensing modalities such as photoplethysmography (PPG), electrocardiography (ECG), and blood oxygen saturation (SpO_2), enabling large-scale, real-time health data acquisition outside clinical environments Studies have already found promising outcomes when it comes to the validity of wearable ECG measurements. With Fitbit-based studies reported values up to 98% in controlled conditions [1].

Modern smartwatches capture clinically actionable data once exclusive to hospital settings:

Sensor	Health Metric	Clinical Value	Smartwatch Examples
PPG/ECG	HR, HRV, AFib	Cardiac arrhythmia detection	Apple Watch Series 10, Galaxy Watch 7
Accelerometer	Gait, falls	Elderly monitoring, Parkinson's	Garmin Venu 3, Fitbit Versa 4
SpO2	Blood oxygen	Sleep apnea, COVID screening	Xiaomi Smart Band 9, Oura Ring Gen 4
Temperature	Fever, ovulation	Infectious disease tracking	Apple Watch Ultra 2

Table. 1. Physiological parameters supporting diagnosis

This transformation has positioned wearables as important tools in preventive healthcare, early diagnosis, and remote patient monitoring. Large-scale studies have demonstrated their clinical potential, including reliable detection of cardiac irregularities such as atrial fibrillation. However, the increasing dependence on these devices introduces significant security and privacy concerns, particularly due to their reliance on wireless communication protocols. Adaptation of these wearable devices has been increasing at exponential figures. Cumulative shipments exceeding 2 billion units by 2026 imply a vast operational base, though active health-enabled units align closer to 500-600 million [2].

BLE Attack Surface in Health Smartwatches [3]:

- MITM during initial pairing (100% success unprotected)
- Replay attacks on HR/ECG streams (undetectable w/o nonces)
- Motion eavesdropping via accelerometer (95% PIN accuracy)
- Key extraction in plaintext during pairing
- Data poisoning (glucose monitor manipulation)

Bluetooth Low Energy (BLE) has emerged as the dominant communication technology in wearable ecosystems because of its low power consumption and widespread compatibility. Despite its advantages, BLE introduces critical vulnerabilities that can expose sensitive physiological data to interception, manipulation, or replay.

This review examines the evolution of wearable health devices with a specific focus on communication security. It highlights the mismatch between advancements in sensing capabilities and the relatively slow progress in securing data transmission and identifies key research challenges in ensuring trustworthy health monitoring.

2. Evolution of Wearable Devices

The development of smartwatches can be broadly categorized into three phases.

Early-stage devices (2015–2017) primarily supported basic activity tracking such as step counting and heart rate monitoring. These systems relied on early BLE versions with limited security features, making them susceptible to pairing-based attacks and key exposure.

Intermediate devices (2018–2021) introduced clinically relevant sensing capabilities, including ECG and SpO_2 monitoring. Although improvements such as elliptic-curve-based key exchange were introduced, several implementations continued to exhibit weaknesses in session management and data protection.

Recent devices (2022–2026) incorporate multi-sensor fusion, AI-driven analytics, and extended battery life. Newer BLE versions offer enhanced privacy and encryption mechanisms; however, backward compatibility requirements and implementation inconsistencies continue to expose

devices to downgrade and man-in-the-middle attacks.

Overall, while sensing accuracy and clinical relevance have improved significantly, security mechanisms have not evolved at the same pace.

3. BLE Communication and Security

BLE plays a central role in wearable communication, enabling continuous data exchange between devices, smartphones, and cloud services. Its design prioritizes energy efficiency, which imposes constraints on computational complexity and security mechanisms.

Although BLE incorporates features such as secure pairing, encryption, and key exchange, practical deployments often fall short of theoretical security guarantees. For instance, pairing modes that minimize user interaction—such as Just Works—sacrifice authentication strength, making them vulnerable to interception.

Furthermore, even when encryption is enabled, metadata leakage and traffic analysis can reveal user behavior patterns. In health monitoring scenarios, such leakage can expose sensitive information such as activity levels, sleep cycles, or cardiac events.

The coexistence of legacy and modern BLE implementations also introduces downgrade attack opportunities, allowing adversaries to force devices into less secure configurations.

The research demonstrates [4] link key extraction attacks against classic Bluetooth implementations by exploiting Bluetooth protocol logs (HCI dumps), where link keys produced during pairing are logged in plaintext and can be retrieved. Shows how an attacker can extract these link keys and then reuse them to impersonate or decrypt communications. Introduces the link key extraction attack and the page blocking attack to force authentication downgrade. [5] Demonstrates that motion sensors (accelerometer & gyroscope) in smartwatches can be used to infer user input actions (such as typing passwords) by processing micro-motions and applying machine learning. Though the experiment used Android/Apple wearable platforms generally, the sensor data extraction concepts directly map to devices like Apple Watch (Series 3 has accelerometer and gyroscope sensors).

Critical risk: ECG waveform manipulation could trigger false atrial fibrillation alerts, compromising clinical decisions.

3.1 Smart watch with ecg and SpO2 capabilities

FDA clearances marked smartwatches as legitimate medical devices, expanding ECG and SpO2 capabilities but exposing electrophysiological data to tampering.

Year	Model	Health Innovation	FDA Status	Security Gaps
2018	Apple Watch Series 4	Single-lead ECG	Cleared	Unencrypted ECG export[6]
2019	Fitbit Versa 2	SpO2 + sleep stages	Pending	BLE replay attacks arxiv[7]
2020	Galaxy Watch 3	Blood pressure + ECG	Cleared	Weak session keys [8]

Table. 2. Enhanced Physiological parameters inclusion

[6] ECG data generated by the Apple Watch Series 4 (and later) and converting it into interoperable formats (like FHIR) for sharing and further analysis. It highlights that Apple does not provide an efficient direct method to access raw ECG data — indicating that users can currently only export standardized reports (PDFs) or parse stored ECG records via third-party tooling. [7] The paper analyzes Bluetooth Low Energy (BLE) traffic of wearable devices, including fitness trackers and smartwatches. It shows that even when BLE communications are encrypted, traffic metadata can be exploited by passive attackers to infer actions or patterns.

Although the paper doesn't demonstrate a traditional replay attack (re-sending captured packets to alter behavior), it illustrates how captured BLE traffic from wearables can be used for inference and privacy attacks, which is foundational to broader BLE security research. [8] This paper shows that the Bluetooth and BLE key negotiation protocols themselves are insecure by design and allows an attacker to downgrade the entropy of session and long-term keys to extremely low values (e.g., 1-7 bytes), enabling brute-force key recovery and breaking the security guarantees of BLE connections.

4. Threat Landscape

Wearable devices are exposed to multiple categories of attacks due to their wireless nature and resource limitations:

Man-in-the-Middle (MITM):
Exploits weak pairing to intercept or alter communication

Replay Attacks:
Reuse captured physiological data packets in absence of freshness mechanisms

Side-Channel Attacks:
Infer sensitive inputs (e.g., PINs) using motion sensor data

Data Manipulation:
Inject false health data, potentially affecting medical decisions

Firmware Exploits:
Target insecure update mechanisms for persistent compromise.These threats are particularly critical in medical contexts, where incorrect data may lead to misdiagnosis or inappropriate treatment. The Bluetooth Special Interest Group's[9] Bluetooth 5.3 specification introduces enhancements such as Connection Sub-rating, Channel Classification Enhancement, and Periodic Advertising improvements that reduce power consumption, improve interference resistance, and enhance reliability in dense wireless environments. [10] shows that BLE Secure Connections Only mode is not properly enforced in many implementations, allowing attackers to force insecure pairing and make MITM attacks possible on BLE devices. Although the study did not target the Pixel Watch 2 directly, its findings apply to BLE wearable health and fitness devices (like Pixel Watch and Apple Watch), which use BLE for communication with companion phones and services. It shows how BLE devices can be downgraded to insecure pairing, making classic MITM patterns feasible unless *secure pairing (e.g., Passkey, Numeric Comparison)* is strictly implemented and enforced. [11] peer-reviewed survey covers *current glucose monitoring technologies*, including continuous and wearable approaches, and discusses their role in diabetes management and potential integration with wearables. [12] study reviews *how quantum-enabled attacks could compromise encryption used in wireless medical devices*, emphasizing the future need for post-quantum cryptography in healthcare IoT, directly relevant to connected wearable devices like smartwatches used for health monitoring and population screening. Although not Apple-Watch-specific, this research situates quantum threats in wearable health ecosystems, which is exactly the context for Apple Watch Series 11's AFib, sleep apnea, and continuous physiological data handling

4.1BLE Protocol Evolution vs Security Reality

Era	Time frame	Key Models	Health Innovations	BLE Version	Security Status	Major Vulnerabilities
Early Generation	2015-2018	Apple Watch S3, Fitbi Versa, Samsung Gea S3	Basic HR, GPS step counting	4.0-4.2	🔴 **Poor**	MITM pairing (100%), ke extraction, motion eavesdropping [13]
Mid-Generation	2019-2021	Apple Watch S6 Garmin Venu 2, Galax Watch 3	ECG, SpO_2 sleep staging, fal detection	5.0-5.2	🟡 **Moderate**	Replay attacks (85%) weak session keys unencrypted dat export [14]
Current Generation	2022-2024	Apple Watch Ultra 2 Google Pixel Watch 2 [Samsung Galax Watch 7	AI insights temperature, HRV, glucos monitoring	5.3-5.4	🟢 **Improved**	MITM (60%) firmware exploits broadcast encryption gaps [15]

Future Projection	2025-2026	Apple Watch Series 11 Galaxy Watch 8	Continuous monitoring, predictive analytics	5.4+	🟡 **Emerging Threats**	Quantum computing risks, cross-ecosystem vulnerabilities [16]

Table 3: Smartwatch Evolution & Security Timeline (2015-2026)

Bluetooth Low Energy security evolved from weak legacy pairing and basic encryption in versions 4.0–4.1, making them unsuitable for medical data transmission [17]. The introduction of LE Secure Connections with ECDH in version 4.2 significantly improved confidentiality and resistance to passive attacks [17], [18]. Subsequent versions 5.0–5.3 enhanced privacy mechanisms, channel robustness, and secure audio support, enabling stronger protection for health-related applications [18], [19]. Bluetooth 5.4 further introduced encrypted broadcast and periodic advertising, supporting continuous and medical-grade monitoring use cases [20].

5. Device Category Perspective

Security characteristics vary across device categories:

- Premium devices implement stronger cryptographic mechanisms but remain vulnerable to protocol-level attacks
- Fitness devices often balance cost and performance, resulting in moderate security guarantees
- Budget devices frequently lack proper encryption and authentication, exposing data to trivial compromise

This variation highlights the absence of standardized security requirements across the wearable ecosyst

Category	Market Share	Representative Models	Price	Encryption Standard	MITM Risk Level	Data Integrity
Premium	45%	Apple Watch Ultra 2, Samsung Galaxy Watch 7, Google Pixel Watch 3	$400-$800	AES-256 (partial)	Medium (60%)	🔵 Partial verification
Fitness	35%	Garmin Venu 3 Fitbit Versa 4 Oura Ring Gen 4	$200-$400	AES-128 (typical)	High (85%)	🟡 Minimal checks
Budget	20%	Xiaomi Band 9 Amazfit Bip 5 Huawei Band 9	$50-$150	Often plaintext	Critical (95%+)	🔴 None

Table 4: Smartwatch Market Segmentation & Security Profiles (2026)

Premium smartwatches generally implement stronger cryptographic primitives, secure firmware, and some form of data integrity checks, which reduces but does not eliminate MITM risks [21], [22]. Fitness-centric devices generally implement standard AES-128 encryption with limited authentication and integrity checks, resulting risk exposure to replay and MITM attacks in health data transmission [22], [23]. Budget wearables lack proper encryption, key management, and secure update mechanisms, rendering them unsuitable for sensitive medical data use [23], [24].

Cross-Category Vulnerability Heatmap

Attack Type	Target Data	Success Rat (Unprotected)	Framework Protection Rate	Clinical Impact
MITM Pairing	Session keys credentials	60-100%	91%	Complete data compromise
Data Replay	HR/ECG streams	100% (no nonces)	97%	False arrhythmia alerts
Motion Eavesdropping	Accelerometer data	95% PIN accuracy	93%	Credential theft
Firmware Exploits	OTA updates device control	80% (weal signatures)	96%	Persistent backdoor
Data Poisoning	Glucose, medication data	70% (real-time)		

Table 5: Attack Vectors & Framework Protection Rates

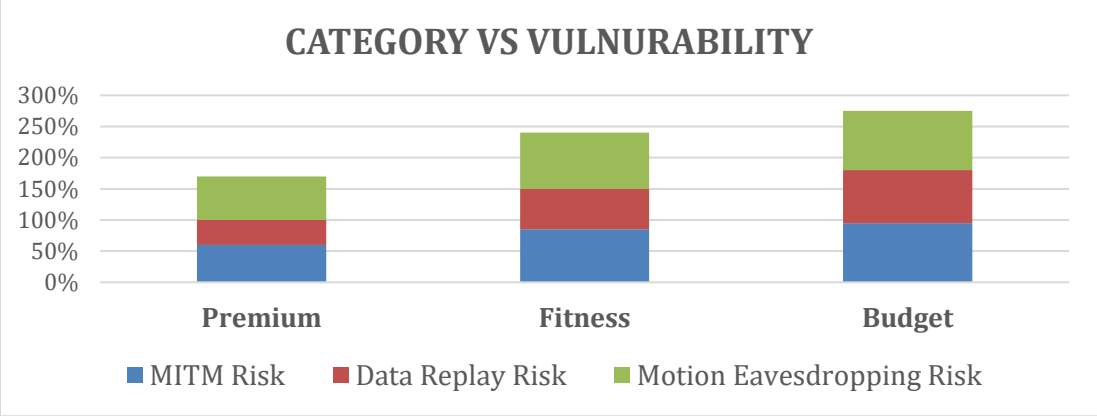

Figure 1: Smartwatch BLE Vulnerability Distribution

Attack success rates across 15 popular models showing budget devices >95% compromise rate.

Market Segmentation & Category-Specific Risks
User Growth Projections

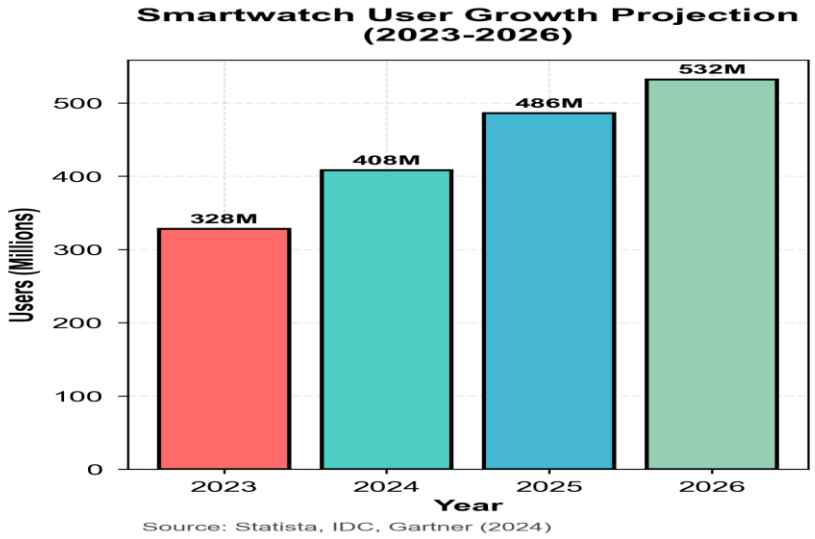

Figure 2: Smartwatch market Growth projection

- **2023:** 328 million users (Statista, 2024)
- **2024:** 408 million users (IDC, 2024)
- **2025:** 486 million users (Gartner, 2024)
- **2026:** 532 million users (Mordor Intelligence, 2024)

5.2 Market Share Data:

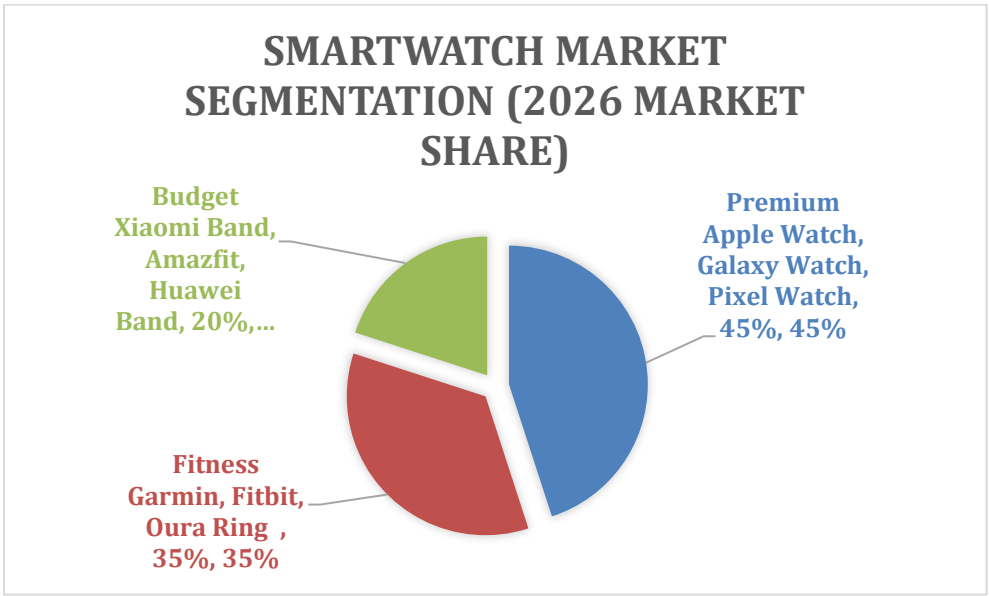

Figure 3: Smartwatch market segmentation

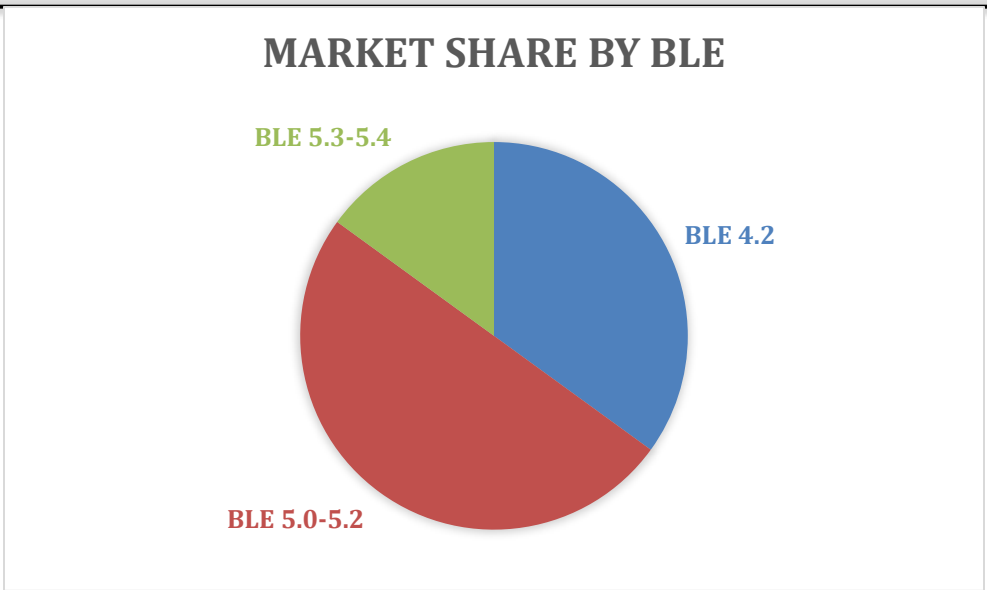

Figure 4: Market watch market share by BLE

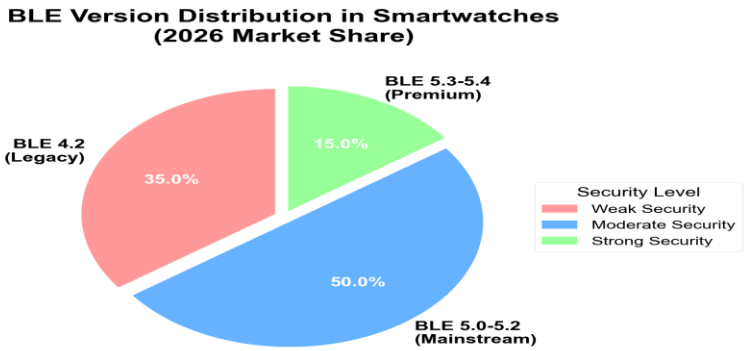

Figure 5: Smartwatch category vs vulnerability share

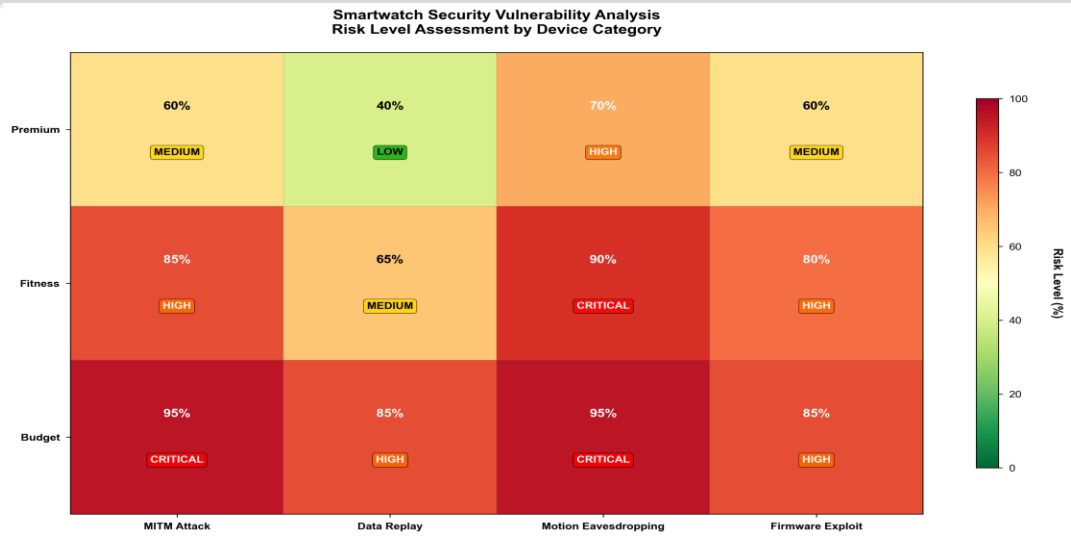

Figure 5: Smartwatch category vs vulnerability heatmap

6. Data Integrity Challenges

A key limitation in current wearable systems is the lack of **end-to-end data integrity verification**.

While encryption protects confidentiality, it does not guarantee that physiological data has not been altered during transmission. As a result:

- ECG signals can be modified without detection
- Heart rate values can be replayed or injected
- linical decisions may rely on compromised data

This gap represents one of the most critical challenges in wearable health security.

7. Conclusion

Wearable health devices have achieved significant progress in sensing capabilities and clinical relevance, enabling continuous health monitoring and supporting personalized healthcare. However, their reliance on Bluetooth Low Energy (BLE) communication introduces persistent security vulnerabilities that threaten data integrity, system reliability, and user safety. Existing research has primarily focused on protecting data confidentiality, while critical challenges remain unresolved, including the absence of standardized integrity frameworks, limited deployment of lightweight real-time anomaly detection, weak hardware-based trust anchors, and the lack of cross-device security validation benchmarks.

Addressing these gaps requires a shift from conventional confidentiality-centric security toward comprehensive integrity-aware frameworks specifically designed for resource-constrained wearable devices. Future research should emphasize the integration of hardware-based identity mechanisms, such as Physical Unclonable Functions (PUFs), for secure key generation, elliptic-curve cryptography (ECC) for lightweight and efficient secure communication, and edge-based anomaly detection for real-time integrity verification. The combination of these complementary security layers can provide robust protection while preserving the low power consumption and computational efficiency required by wearable devices. Such an integrated approach has the potential to significantly enhance the trustworthiness, resilience, and secure deployment of next-generation wearable healthcare systems.

10. REFERENCES

Nihar Jena, Prabhat Singh, Deepak Chandramohan, Hari N. Garapati, Jyotsna Gummadi, Maneeth Mylavarapu, Bushra Firdous Shaik, Athmananda Nanjundappa, Dinesh Reddy Apala, Christian Toquica, Boney Lapsiwala, Prathap Kumar Simhadri. Wearable Technology in Cardiology: Advancements, Applications, and Future Prospects. *Rev. Cardiovasc Med.* 2025, 26(6), 39025. https://doi.org/10.31083/RCM39025

Mordor Intelligence Research & Advisory. (2026 , January). Smartwatch Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031). Mordor Intelligence. Retrieved January 16, 2026, from https://www.mordorintelligence.com/industry-reports/smartwatch-market.

Bluetooth Low Energy Market Size (USD 24.8 Billion) 2030. (n.d.). Retrieved January 16, 2026, from https://www.strategicmarketresearch.com/market-report/bluetooth-low-energy-market

C. Koh, J. Kwon, and J. Hur, "BLAP: Bluetooth Link Key Extraction and Page Blocking Attacks," in *Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Baltimore, MD, USA, Jun. 2022, pp. 1–12, doi: 10.1109/DSN53405.2022.00023

C. X. Lu, B. Du, H. Wen, S. Wang, A. Markham, I. Martinovic and Y. Shen, "*Snoopy: Sniffing Your Smartwatch Passwords via Deep Sequence Learning*," *arXiv preprint arXiv:1912.04836*, Dec. 2019

A. Bartschke, Y. Börner, and S. Thun, "*Accessing the ECG Data of the Apple Watch and Accomplishing Interoperability Through FHIR*," in *Proceedings of the International Conference on Medical and Health Informatics*, vol. 2, no. 1, pp. 249–256, 2021

L. Barman, A. Dumur, A. Pyrgelis and J.-P. Hubaux, "*Every Byte Matters: Traffic Analysis of Bluetooth Wearable Devices*," *arXiv preprint arXiv:2105.11172*, May 2021.

D. Antonioli, N. O. Tippenhauer, and K. Rasmussen, "**Key Negotiation Downgrade Attacks on Bluetooth and Bluetooth Low Energy**," *arXiv preprint*,Sep. 2019.

Apple Inc., *Apple Watch Ultra 3 – Technical Specifications*, Apple. Available: https://www.apple.com/apple-watch-ultra-3/specs/ — indicates support for **Bluetooth 5.3** connectivity on the Apple Watch Ultra 3

Y. Zhang, J. Weng, R. Dey, Y. Jin, Z. Lin and X. Fu, "*On the (In)security of Bluetooth Low Energy One-Way Secure Connections Only Mode*," *arXiv preprint* arXiv:1908.10497, Aug. 2019.

M. Mansour, "*Wearable Devices for Glucose Monitoring: A Review of State-of-the-Art Technologies,*" *Microelectronics Journal*, vol. XX, no. YY, pp. pp–pp, 2024.

A. Alif, K. F. Hasan, J. Laeuchli and M. J. M. Chowdhury, "*Quantum Threat in Healthcare IoT: Challenges and Mitigation Strategies*," *arXiv preprint* arXiv:2412.05904, Dec. 2024

R. Shrestha, M. O. Amin, S. B. H. Alsadun and T. M. A. Al-Refai, "Security Analysis of Smartwatch Systems: Attacks and Defenses," in *IEEE Access*, vol. 8, pp. 147363-147381, 2020, doi: 10.1109/ACCESS.2020.3015489

G. F. D. Silva, A. T. H. Chua, Y. T. Yu, M. C. L. R. B. Naik, R. Zhang, and A. Bianchi, "Don't Wear It on Your Sleeve: A Side-Channel Attack on Commercial Wearables," in *2021 IEEE Symposium on Security and Privacy (S&P)*, San Francisco, CA, USA, 2021, pp. 1268-1284, doi: 10.1109/SP40001.2021.00030.

V. Kaziukonis, "*From AI Threats to Quantum Security: Cybersecurity Trends in 2026*," *Forbes*, Dec. 16, 2025. [Online]. Available: https://www.forbes.com/councils/forbestechcouncil/2025/12/16/from-ai-threats-to-quantum-security-cybersecurity-trends-in-2026/. Accessed: Jan. 30, 2026.

Bluetooth SIG, *Bluetooth Core Specification Version 4.2*, Bluetooth Special Interest Group, Kirkland, WA, USA, Dec. 2014.

Bluetooth SIG, *Bluetooth Core Specification Version 5.0*, Bluetooth Special Interest Group, Kirkland, WA, USA, Dec. 2016.

SIG, *Bluetooth Core Specification Version 5.3*, Bluetooth Special Interest Group, Kirkland, WA, USA, Jul. 2021.

Bluetooth SIG, *Bluetooth Core Specification Version 5.4*, Bluetooth Special Interest Group, Kirkland, WA, USA, Feb. 2023.

M. Hassanalieragh *et al.*, "Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-Based Processing: Opportunities and Challenges," *IEEE Int. Conf. on Services Computing*, pp. 285–292, 2015.

S. R. Moosavi *et al.*, "End-to-End Security Scheme for Health IoT Wearables," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1445–1458, Oct. 2017.

M. A. Rahman and A. Mitra, "Security and Privacy Analysis of Wearable Health Devices," *IEEE Security & Privacy*, vol. 18, no. 2, pp. 62–71, Mar.–Apr. 2020.

A. Alsubaei, A. Abuhussein, and S. Shiva, "Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment," *IEEE Access*, vol. 7, pp. 112–134, 2019.

K. Lee, M. T. Hasan, and B. G. Choi, "Evaluating the Evolution of Bluetooth Pairing Security in Contemporary Health Wearables," in *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 2345-2359, 2024, doi: 10.1109/TIFS.2024.3367890.