

Wearable Biomedical Monitoring Systems for Occupational Health: A Scoping Review of Technologies, Applications, Privacy Risks, and Cybersecurity Challenges (2020–2026) [†]

Laura Cătălina Dospinescu ^{*}, Laurențiu Dan Milici , Edi Marian Timofte  and Marcel Pușcașu 

Department of Computers, Automation and Electronics, Stefan cel Mare University of Suceava, 720229 Suceava, Romania; dam@usm.ro (L.D.M.); edi.timofte@usm.ro (E.M.T.); marcel.puscasu@student.usv.ro (M.P.)

^{*} Correspondence: laurad@usm.ro; Tel.: +40-755-223-670

[†] Presented at the International Conference on Electromagnetic Fields, Signals and BioMedical Engineering (ICEMS-BIOMED), Suceava, Romania, 7–9 May 2026.

Abstract

Smart wearable biomedical sensors/devices provide the ability for continuous monitoring of physiological parameters in occupational settings. Industrial Internet of Things (IIoT)'s integration in wearable biomedical technology presents additional cybersecurity risks and privacy concerns as attack surfaces expand and sensitive biometric data is processed. This scoping review included studies published between 2020 and 2026, screened according to PRISMA-ScR guidelines, which identified 39 articles. The findings indicate that most systems rely on commercial wearables for monitoring fatigue, stress, and environmental conditions, often with limited consideration of the cybersecurity aspects. Common risks include insecure wireless communication, data interception, firmware and supply chain attacks, and vulnerabilities related to IT/OT integration. To address these challenges, this study proposes a multi-layer threat taxonomy covering sensing, communication, processing, AI/analytics, and organizational layers. The results highlight the need for end-to-end cyber-resilient architectures and privacy-by-design approaches in occupational wearable monitoring systems.

Keywords: cybersecurity; cyber-physical systems; IIoT; occupational health monitoring; privacy protection; threat taxonomy; wearable biomedical sensors; worker fatigue detection

1. Introduction

Wearable technologies have greatly changed how occupational health can be monitored due to their rapidly developing nature [1–4].

The increased use of wearable monitoring technologies was primarily driven by the growth of the Internet of Things (IoT), particularly the Industrial Internet of Things (IIoT). In IIoT, wearable devices act as distributed sensor nodes, collecting physiological data and sending the information to edge or cloud computing platforms where complex analyses and decision-making tools can be utilized [5–8].

Despite the significant opportunity wearable biomedical monitoring technology presents, there are numerous technical, ethical, and regulatory barriers to deploying wearable monitoring technology in workplace settings. The continuous collection of physiological signals will generate large amounts of sensitive biometric data that must be collected, transmitted, stored, and processed in a secure manner. When this sensitive data is improp-



Academic Editors: L. Dan Milici,
Mihai Munteanu, Simona Miclăuș,
Paul Bechet and Radu Ciorap

Published: 14 July 2026

Copyright: © 2026 by the authors.
Licensee MDPI, Basel, Switzerland.
This article is an open access article
distributed under the terms and
conditions of the [Creative Commons
Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

erly secured, it creates the potential for privacy violations, unauthorized surveillance, or misuse of personal health information [9] by others.

In addition to the privacy concerns, wearable biomedical monitoring technology also presents new cybersecurity risks. Wearable devices commonly utilize wireless communication technologies such as Bluetooth Low Energy (BLE), Wi-Fi, or proprietary IoT protocols, which create vulnerabilities such as insecure pairing procedures, eavesdropping attacks, replay attacks, and device spoofing [10–14].

One of the other key issues relates to the regulatory and ethical implications of collecting physiological data from employees. Wearable monitoring systems commonly employed in workplaces generally fall outside of the rigorous regulatory frameworks that govern the collection and protection of healthcare data [15]. Regulatory ambiguity surrounding the collection of employee biometric and physiological data raises questions relating to employee consent, transparency, data ownership, and the potential exploitation of employee biometric data through the use of wearable monitoring technologies.

Although wearable biomedical monitoring technologies have received considerable attention in recent years, most of the existing research has focused primarily on the development of sensors, the analysis of physiological signals, and/or particular occupational health applications. There are not many studies that look at how wearable devices affect the security and privacy of Industrial Internet of Things systems.

This study addresses this gap by conducting a systematic scoping review of literature on occupational wearable biomedical monitoring systems, published between 2020 and 2026. Furthermore, a multi-layer threat taxonomy is proposed, covering sensing, communication, processing, AI-model, and organizational layers. We will also summarize what other people have found out and propose a way to classify security threats, which we call a multi-layer threat taxonomy. That will help us understand the problems that can happen in these systems, including devices that can sense things networks cannot, and engines that analyze data and organize it based on a set of rules.

2. Methodology

In this case, a scoping review was chosen to map the research landscape of wearable biomedical monitoring technologies in occupational settings and to determine the cybersecurity and privacy concerns associated with those technologies [16–21].

To accomplish this objective, a systematic and structured review methodology will be utilized, and the PRISMA-ScR methodology will serve as the foundation for the review process [22]. The PRISMA-ScR methodology is specifically designed for the purpose of conducting a systematic review of a wide range of topics, including those in emerging technology areas where there are many different experimental designs, technologies, and evaluation approaches employed [23].

Research Questions

The research questions examined in this study are defined as follows:

- RQ1: What types of wearable biomedical monitoring technologies are used in occupational settings?
- RQ2: What physiological and safety parameters are monitored?
- RQ3: What cybersecurity and privacy risks are associated with these systems?
- RQ4: What mitigation strategies have been proposed?

A systematic search was conducted across Web of Science, Scopus, IEEE Xplore, PubMed, and ScienceDirect.

The search strategy was also developed to identify studies published from January 2020 through March 2026, since these represent the timeframe over which wearable moni-

toring technology has rapidly evolved and the need for cybersecurity within connected health systems has increased [20].

The search used combinations of keywords related to wearable devices, occupational monitoring, IoT, and cybersecurity. An example query is:

("sensors" OR "wearable devices" OR "biomedical wearables") AND ("occupational health" OR "worker monitoring" OR "workplace safety") AND ("IoT" OR "industrial IoT" OR "cyber-physical systems") AND ("cybersecurity" OR "security" OR "privacy" OR "data protection") [21].

The researchers performed the study selection according to the PRISMA-ScR framework, which involved four primary steps: identification, screening, eligibility evaluation, and final inclusion.

More than 1200 articles were initially retrieved by the researchers through the database searches. This initial list was then reduced by eliminating duplicates and performing a title/abstract screening based on the relevance of these articles to wearable monitoring and occupational health applications.

After the screening phase, the remaining studies underwent an eligibility phase in which the full-text articles were reviewed against the previously established inclusion/exclusion criteria in relation to wearable monitoring systems used in occupational environments, as well as the security and privacy issues of these systems.

Data were extracted and categorized based on device types, monitored parameters, application domains, system architectures, identified vulnerabilities, and mitigation strategies. The analysis supported the development of the proposed multi-layer threat taxonomy [21,22]. No formal critical appraisal was performed, consistent with the scoping review methodology [23,24]. The synthesis combined narrative description with quantitative summaries (e.g., frequencies of device types and domains) and thematic categorization to inform the proposed taxonomy [24,25].

3. Results

Study Selection

The search was conducted using a systematic approach according to the PRISMA-ScR guidelines with the searching of PubMed, Scopus, Web of Science, IEEE Xplore, and ScienceDirect databases. A total of 1208 relevant papers from the years 2020 to 2026 were found. Upon removing duplicate papers, 842 papers that had been screened at the title and abstract level were reviewed as full text. From this full-text review, 214 papers were evaluated for eligibility, based upon the established criteria for inclusion/exclusion. As a result, a total of 68 studies met the established criteria and were therefore included in the qualitative synthesis. The major reasons for exclusion during full-text reviews were the lack of clear discussion on the privacy/cybersecurity aspects of a study ($n = 89$), a study focused exclusively on non-occupational use (e.g., consumer/sports-related applications) ($n = 37$), or there was an insufficient number of technical details regarding the system's architecture/security design ($n = 20$). A total of 68 studies were ultimately synthesized in accordance with the PRISMA flow diagram, shown in Figure 1.

Most of the included studies ($\approx 65\%$, $n = 44$) were published between 2022 and 2025. Experimental prototypes and field trials dominated the literature ($\approx 72\%$, $n = 49$), while the remaining studies consisted of reviews and analytical frameworks. Commercial or semi-commercial wearable devices represented the majority of technologies ($\approx 62\%$, $n = 42$), with the rest being custom multi-sensor prototypes [3,25–29].

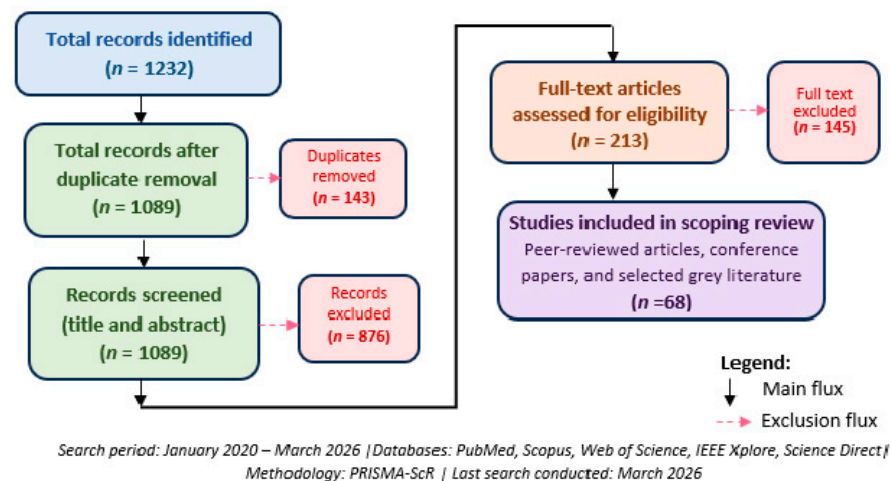


Figure 1. PRISMA 2020 flow diagram (adapted for this scoping review following the PRISMA-ScR extension) illustrating the identification, screening, eligibility assessment, and inclusion of sources on wearable biomedical monitoring systems for occupational health with cybersecurity and privacy considerations (2020–2026).

The identified wearable sensor technologies include:

- Physiological sensors ($\approx 45\%$, $n = 31$)—HR/HRV via PPG/ECG;
- Motion sensors ($\approx 38\%$, $n = 26$)—IMU-based posture and activity tracking;
- Environmental sensors ($\approx 22\%$, $n = 15$)—temperature and gas monitoring;
- Advanced sensors ($\approx 12\%$, $n = 8$)—EEG and eye-tracking;
- Multi-sensor platforms ($\approx 18\%$, $n = 12$)—integrated monitoring systems.

Frequently monitored parameters include:

- Heart rate/HRV ($\approx 68\%$, $n = 46$);
- Motion and posture ($\approx 55\%$, $n = 37$);
- Body temperature ($\approx 32\%$, $n = 22$);
- Stress indicators and SpO_2 ($\approx 15\text{--}18\%$, $n = 10\text{--}12$);
- Composite fatigue indices ($\approx 25\%$, $n = 17$);
- Environmental parameters ($\approx 28\%$, $n = 19$).

Applications were concentrated in high-risk sectors:

- Construction ($\approx 35\%$, $n = 24$);
- Manufacturing ($\approx 28\%$, $n = 19$);
- Mining ($\approx 18\%$, $n = 12$);
- Logistics ($\approx 12\%$, $n = 8$);
- Other domains ($\approx 7\%$, $n = 5$).

Most systems ($\approx 75\%$, $n = 51$) adopted hybrid IIoT architectures, combining BLE/Wi-Fi communication ($\approx 82\%$), edge processing ($\approx 45\%$), and cloud analytics ($\approx 68\%$). Fully edge-based solutions remained limited ($\approx 12\%$), mainly in privacy-sensitive scenarios.

4. Cybersecurity and Privacy Challenges

Wearable biomedical monitoring systems improve occupational safety but introduce significant cybersecurity and privacy risks due to continuous data collection, wireless communication, and integration into IIoT environments [11,30].

Studies from 2020 to 2026 have repeatedly identified similar security vulnerabilities in wearable and IoT-based health monitoring systems employed in various industrial applications:

- Insecure wireless communication: BLE ($\approx 82\%$ of architectures) is vulnerable to eavesdropping, MITM, replay, and spoofing attacks due to weak pairing and encryption mechanism [3,31].
- Firmware and supply chain risks: OTA updates and supply chain attacks can enable persistent compromise and unauthorized access to physiological data [32,33].
- Device-level weaknesses: Limited resources often prevent strong authentication, secure boot, or intrusion detection, making devices vulnerable to tampering, side-channel attacks, and DoS [34].
- OT/IT convergence risks: Integration with ICS/SCADA systems allows compromised wearables to be used for lateral movement, potentially impacting operational safety [28,33].

Approximately 65% of studies reported communication-layer vulnerabilities, while 40% highlighted firmware and supply chain risks [32]. Wearables are particularly exposed in harsh industrial environments with limited maintenance conditions [25].

Continuous monitoring of sensitive biometric data (e.g., heart rate variability, movement patterns, and body temperature) enables the creation of detailed worker profiles, raising significant privacy concerns [34,35]:

- Surveillance and data misuse: Wearable systems may enable excessive monitoring beyond safety purposes, leading to productivity tracking, discrimination, and misuse of employee data [34,36].
- Lack of informed consent and transparency: Many occupational wearables fall outside strict medical regulations, resulting in unclear consent mechanisms and ambiguous data ownership [15,36].
- Re-identification and profiling risks: Aggregated datasets may allow re-identification of individuals, even when anonymization techniques are applied, raising concerns under privacy regulations such as GDPR [31,37].
- Regulatory ambiguity: Occupational wearables often operate outside healthcare-specific frameworks, creating compliance challenges across jurisdictions [15].
- User acceptance and trust issues: Approximately 55% of studies report ethical concerns related to surveillance and consent, which may limit adoption in high-risk environments [37].

Compromised wearable systems may not only expose sensitive data but also affect safety monitoring integrity, for example through manipulated fatigue alerts or undetected overload conditions [11]. The convergence of OT/IT networks amplifies these risks, turning individual device vulnerabilities into systemic threats to industrial processes [33].

5. Proposed Multi-Layer Threat Taxonomy

This study proposes a multi-layer threat taxonomy for analyzing cybersecurity and privacy risks in occupational wearable biomedical monitoring systems within IIoT environments. As shown in Figure 2, the taxonomy divides threats into five interconnected layers—sensing, communication, processing, AI-model/analytics, and organizational—representing each stage of the end-to-end data life cycle, from the wearable device to organizational decision-making. The layered model provides an additional dimension beyond current IoT and IIoT security frameworks that are focused on worker safety (device failure impacts real-time monitoring integrity) and privacy (continuous biometric data collection in unclear regulatory contexts) [36,37].

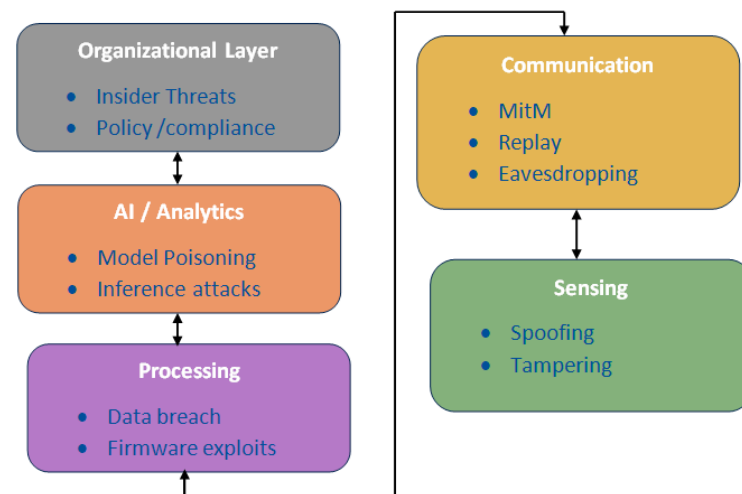


Figure 2. A proposed threat taxonomy for occupational wearable biomedical monitoring system organized in multiple layers such as sensing, communication, processing, AI-model/analytics, and organizational layers. The various forms of attack vectors and propagation paths are illustrated in each layer.

Sensing layer: Threats target physical wearable devices and embedded sensors (e.g., PPG, IMU, temperature). These include sensor spoofing, physical tampering, calibration attacks, and side-channel leakage, which can compromise data integrity and lead to incorrect safety assessments [3,35].

Communication layer: Includes eavesdropping, Man-in-the-Middle, replay attacks, jamming, and insecure pairing methods, which can expose or manipulate sensitive physiological data and enable unauthorized surveillance [3,28].

Processing layer: Covers edge and cloud platforms, where threats include firmware exploits, unauthorized access, data breaches, resource exhaustion, and supply chain attacks, potentially affecting system reliability and causing large-scale privacy exposure [28,33].

AI/analytics layer: Includes adversarial threats such as model poisoning, model inversion, inference attacks, and backdoors, which may lead to biased predictions or manipulated safety decisions [11,26].

Organizational layer: Encompasses governance and human factors, including insider threats, weak consent mechanisms, regulatory non-compliance, and social engineering risks, potentially resulting in privacy violations and reduced user trust [34,37].

This taxonomy enables structured risk analysis and supports the design of resilient security mechanisms across the wearable monitoring life cycle.

6. Security and Privacy Mitigation Strategies

In terms of mitigating the privacy and security concerns associated with occupational wearable monitoring systems, the existing body of research includes several strategies that have been proposed to help alleviate these concerns. However, it is important to note that, while there is a wide array of strategies being proposed, the actual implementation of many of these strategies continues to vary greatly, and much of the strategy proposals remain in the theoretical/prototype phase. Additionally, by mapping the proposed strategies to the multi-layered taxonomy developed in Section 5 above, we can provide an additional framework for developing cyber-resilient designs.

A number of strategies have been identified at the sensing layer, which include: hardware-based protection mechanisms (i.e., tamper resistant enclosures, secure boot processes and sensor calibration verification) to protect against spoofing or tampering of the sensors themselves [35,38]; and, for wearables that are resource constrained, lightweight

cryptographic primitives (for example Elliptic Curve Cryptography) and Trusted Execution Environments (TEEs) may be used to protect against side-channel attacks [39].

End-to-end encryption; mutual authentication prior to pairing; secure key exchange protocols (for example DTLS for Bluetooth Low Energy); and, anomaly detection for traffic patterns have emerged as some of the most common strategies for protecting against eavesdropping, Man-in-the-Middle (MITM), and replay attacks in the communication layer [3,28]. In addition, a number of studies suggest that the use of “protocol hardening” (for example randomized MAC addresses and frequency hopping) should be employed, especially in industrial environments where jamming is more likely to occur [12].

Secure enclaves at edge gateways; data-at-rest encryption; and, access control lists to limit who has access to aggregated datasets represent some of the ways that the processing layer may employ zero trust architectures [33,39]. Federated learning approaches also exist, and they allow for sensitive physiological data to remain on devices or edge nodes and reduce cloud exposure, thereby providing for privacy-preserving analytics [37].

For the AI/model/analytics layer, the defense strategies include: adversarial training; model watermarking; differential privacy techniques; and, runtime monitoring to identify poisoning or inference attacks [11,32]. Explainable AI methods are also recommended to increase transparency into how fatigue prediction models arrive at certain conclusions, thereby increasing the auditability of the process and reducing the potential for discriminatory results [26].

Finally, the organizational layer defense strategies include: privacy-by-design principles (such as data minimization, purpose limitation, and regular privacy impact assessments); clearly defined consent frameworks; education programs for workers; and, policies that clearly prohibit non-safety uses of monitoring data [34,37]. Regulatory alignment, including extending protections afforded under laws like GDPR to non-medical occupational wearables, is often called for to resolve ambiguities and hold accountable those who collect and use this type of data [15,36].

Methods suggested by prior works can be categorized using the taxonomy above. Methods at the sensing level include physical unclonable functions, secure booting, and lightweight cryptography. Some methods exist at the communication level, such as end-to-end encryption, mutual authentication, and communication protocol hardening.

Methods at the processing/storage layer include zero trust architectures, data encryption and anonymization, and federated learning approaches which provide security for aggregated data. Prior work had also suggested methods which can be applied at the AI/analytics level, such as adversarial training, differential privacy, and explainable AI. Privacy-by-design, consent frameworks, and regulatory approaches exist for the organizational level.

While there are mitigation methods for most stages of IoT systems, many of these methods are not well implemented past the design or proof-of-concept stages, and there are few examples of end-to-end solutions deployed within occupational settings.

7. Discussion and Research Directions

This review highlights the rapid development of wearable monitoring systems alongside significant gaps in cybersecurity and privacy protection.

The proposed multi-layer taxonomy provides a structured framework for analyzing risks across the entire data life cycle.

In practice, organizations face trade-offs between real-time safety monitoring and the protection of sensitive employee data. Poor transparency and weak consent mechanisms may limit adoption, particularly in high-risk environments [15,34,36,37].

Technically, the study identifies considerable progress in layer-specific countermeasures (Section 6); specifically, end-to-end encryption, federated learning, and differential privacy. However, there is very little evidence of fully integrated end-to-end countermeasures that have been tested in operational conditions in occupational environments. The majority of countermeasures are either conceptual or prototype-based and do not address multi-layered attack chains or the extreme environment conditions of industrial workplaces (dust, vibrations, etc., and limited connectivity).

Important limitations of this review include that it was only able to consider English-language published works and the gray/peer-reviewed literature that could be accessed via main databases, therefore possibly omitting reports from other regions or internal reports from various industries. In accordance with the scoping methodology [23,24], the lack of formal quality appraisal prioritized scope over detail and therefore may overlook methodological deficiencies in primary studies.

Research efforts in the next few years should primarily be focused on:

- Development of full-stack cyber-resilient solutions validated in real environments;
- Evaluation of user trust, consent mechanisms, and transparency;
- Extension of privacy regulations to occupational wearables;
- Investigation of emerging threats (e.g., adversarial ML, quantum-resistant cryptography);
- Interdisciplinary research integrating cybersecurity, occupational health, and human factors.

Key areas for research can be organized based on time scales over which they can make progress.

Immediate: Validating fixes for known vulnerabilities, improving defenses such as secure coding techniques, and strengthening authentication.

Near future: Creating converged security architectures, expanding industry compliance standards, and defining trusted data formats.

Future: Advancing future proofing technologies such as quantum crypto-analysis, human–cyber–physical systems, etc.

8. Conclusions

Occupational wearable biomedical monitoring systems have shown great promise during 2020–2026 as a safety-enhancing technology, but they also raise concerns regarding cybersecurity and privacy.

Applications of wearables are rapidly growing in IIoT-based systems, yet the security aspects of these systems have not been prioritized and remain vulnerable to attacks. Common security concerns range from insecure communications to firmware tampering and information misuse. Privacy issues include employee monitoring, transparency, and regulatory concerns.

We introduce a threat taxonomy that categorizes threats into sensing, communication, processing, AI/analytics, and organizational layers.

Most proposed solutions focus on individual layers and are at a prototype stage. Therefore, there is a critical need for collaborative real-world cyber-resilient solutions.

Research gaps include the need for end-to-end secure systems architectures, better regulation, and the human factors of trust, transparency, and acceptance.

Author Contributions: Conceptualization, L.C.D. and E.M.T.; Methodology, L.C.D., L.D.M., E.M.T. and M.P.; Validation, E.M.T. and L.D.M.; Investigation, L.C.D., E.M.T. and M.P.; Resources, L.C.D. and E.M.T.; Writing—original draft, L.C.D. and E.M.T.; Visualization, E.M.T.; Supervision, L.D.M.; Project administration, E.M.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available upon request from the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
BLE	Bluetooth Low Energy
DoS	Denial of Service
DTLS	Datagram Transport Layer Security
ECG	Electrocardiogram
EEG	Electroencephalography
GDPR	General Data Protection Regulation
GSR	Galvanic Skin Response
HIPAA	Health Insurance Portability and Accountability Act
HR	Heart Rate
HRV	Heart Rate Variability
ICS	Industrial Control Systems
IIoT	Industrial Internet of Things
IMU	Inertial Measurement Unit
IoMT	Internet of Medical Things
IoT	Internet of Things
IT	Information Technology
MAC	Media Access Control
MITM	Man-in-the-Middle
ML	Machine Learning
OT	Operational Technology
OTA	Over-the-Air
PPG	Photoplethysmography
OWM	Occupational Worker Monitoring
PRISMA-ScR	Preferred Reporting Items for Systematic Reviews and Scoping Reviews
SCADA	Supervisory Control and Data Acquisition
SpO ₂	Peripheral Capillary Oxygen Saturation
TEE	Trusted Execution Environment

References

1. Bonato, P. Wearable Sensors and Systems. *IEEE Eng. Med. Biol. Mag.* **2010**, *29*, 25–36. [\[CrossRef\]](#) [\[PubMed\]](#)
2. Haghi, M.; Thurow, K.; Stoll, R. Wearable Devices in Medical Internet of Things: Scientific Research and Commercially Available Devices. *Healthc. Inform. Res.* **2017**, *23*, 4–15. [\[CrossRef\]](#) [\[PubMed\]](#)
3. Svertoka, E.; Saafi, S.; Rusu-Casandra, A.; Burget, R.; Marghescu, I.; Hosek, J.; Ometov, A. Wearables for Industrial Work Safety: A Survey. *Sensors* **2021**, *21*, 3844. [\[CrossRef\]](#) [\[PubMed\]](#)
4. Patel, S.; Park, H.; Bonato, P.; Chan, L.; Rodgers, M. A review of wearable sensors and systems with application in rehabilitation. *J. Neuroeng. Rehabil.* **2012**, *9*, 21. [\[CrossRef\]](#) [\[PubMed\]](#)
5. Xu, L.D.; He, W.; Li, S. Internet of Things in Industries: A Survey. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2233–2243. [\[CrossRef\]](#)
6. Boyes, H.; Hallaq, B.; Cunningham, J.; Watson, T. The industrial internet of things (IIoT): An analysis framework. *Comput. Ind.* **2018**, *101*, 1–12. [\[CrossRef\]](#)
7. Zhou, K.; Liu, T.; Zhou, L. Industry 4.0: Towards future industrial opportunities and challenges. In *2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*; IEEE: New York, NY, USA, 2015; pp. 2147–2152. [\[CrossRef\]](#)
8. Tao, F.; Qi, Q.; Liu, A.; Kusiak, A. Data-driven smart manufacturing. *J. Manuf. Syst.* **2018**, *48*, 157–169. [\[CrossRef\]](#)

9. Ajunwa, I.; Crawford, K.; Schultz, J. Limitless Worker Surveillance. *Calif. Law Rev.* **2017**, *105*, 735. [\[CrossRef\]](#)
10. Ryan, M. Bluetooth: With low energy comes low security. In Proceedings of the 7th USENIX Conference on Offensive Technologies (WOOT'13), Washington, DC, USA, 13 August 2013; p. 4.
11. Zhang, B.; Chen, C.; Lee, I.; Lee, K.; Ong, K.-L. A survey on security and privacy issues in wearable health monitoring devices. *Comput. Secur.* **2025**, *155*, 104453. [\[CrossRef\]](#)
12. Sadhu, P.K.; Yanambaka, V.P.; Abdelgawad, A. Internet of Things: Security and Solutions Survey. *Sensors* **2022**, *22*, 7433. [\[CrossRef\]](#) [\[PubMed\]](#)
13. Knapp, E.D. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*; Elsevier: Amsterdam, The Netherlands, 2024.
14. Zhai, B.; Akande, O.N.; Agarwal, S.; Pak, W. Security risk assessment of internet of things health devices using DREAD and STRIDE models. *Ain Shams Eng. J.* **2025**, *16*, 103721. [\[CrossRef\]](#)
15. Voigt, P.; Von Dem Bussche, A. *The EU General Data Protection Regulation (GDPR)*; Springer International Publishing: Cham, Switzerland, 2017. [\[CrossRef\]](#)
16. Arksey, H.; O'Malley, L. Scoping studies: Towards a methodological framework. *Int. J. Soc. Res. Methodol.* **2005**, *8*, 19–32. [\[CrossRef\]](#)
17. Munn, Z.; Peters, M.D.J.; Stern, C.; Tufanaru, C.; McArthur, A.; Aromataris, E. Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. *BMC Med. Res. Methodol.* **2018**, *18*, 143. [\[CrossRef\]](#) [\[PubMed\]](#)
18. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; Keele University: Staffordshire, UK; Durham University: Durham, UK, 2007.
19. Kitchenham, B.; Pretorius, R.; Budgen, D.; Brereton, O.P.; Turner, M.; Niazi, M.; Linkman, S. Systematic literature reviews in software engineering—A tertiary study. *Inf. Softw. Technol.* **2010**, *52*, 792–805. [\[CrossRef\]](#)
20. Webster, J.; Watson, R.T. Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Q.* **2002**, *26*, xiii–xxiii. [\[CrossRef\]](#)
21. Snyder, H. Literature review as a research methodology: An overview and guidelines. *J. Bus. Res.* **2019**, *104*, 333–339. [\[CrossRef\]](#)
22. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ* **2021**, *372*, n71. [\[CrossRef\]](#) [\[PubMed\]](#)
23. Kitchenham, B. *Procedures for Performing Systematic Reviews*; Keele University: Staffordshire, UK; National ICT Australia Ltd.: Sydney, Australia, 2004; Volume 33, pp. 1–26.
24. Brereton, P.; Kitchenham, B.A.; Budgen, D.; Turner, M.; Khalil, M. Lessons from applying the systematic literature review process within the software engineering domain. *J. Syst. Softw.* **2007**, *80*, 571–583. [\[CrossRef\]](#)
25. Naranjo, J.E.; Mora, C.A.; Villagómez, D.F.B.; Falconi, M.G.M.; Garcia, M.V. Wearable Sensors in Industrial Ergonomics: Enhancing Safety and Productivity in Industry 4.0. *Sensors* **2025**, *25*, 1526. [\[CrossRef\]](#) [\[PubMed\]](#)
26. Aksüt, G.; Eren, T.; Alakaş, H.M. Using wearable technological devices to improve workplace health and safety: An assessment on a sector base with multi-criteria decision-making methods. *Ain Shams Eng. J.* **2024**, *15*, 102423. [\[CrossRef\]](#)
27. Moon, J.; Ju, B.-K. Wearable Sensors for Healthcare of Industrial Workers: A Scoping Review. *Electronics* **2024**, *13*, 3849. [\[CrossRef\]](#)
28. Bhatti, D.S.; Saleem, S.; Imran, A.; Iqbal, Z.; Alzahrani, A.; Kim, H.; Kim, K.-I. A Survey on Wireless Wearable Body Area Networks: A Perspective of Technology and Economy. *Sensors* **2022**, *22*, 7722. [\[CrossRef\]](#) [\[PubMed\]](#)
29. Shojaei, P.; Vlahu-Gjorgievska, E.; Chow, Y.-W. Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review. *Computers* **2024**, *13*, 41. [\[CrossRef\]](#)
30. Khan, A.; Duncan, D. Remote Patient Monitoring Applications in Healthcare: Lessons from COVID-19 and Beyond. *Electronics* **2025**, *14*, 3084. [\[CrossRef\]](#)
31. Pool, J.; Akhlaghpour, S.; Fatehi, F.; Burton-Jones, A. A systematic analysis of failures in protecting personal health data: A scoping review. *Int. J. Inf. Manag.* **2024**, *74*, 102719. [\[CrossRef\]](#)
32. Okonkwo, C.; Awolusi, I.; Nnaji, C.; Akanfe, O. Privacy and security of wearable internet of things: A scoping review and conceptual framework development for safety and health management in construction. *Comput. Secur.* **2025**, *150*, 104275. [\[CrossRef\]](#)
33. Virgillito, D.; Catalfo, P.; Ledda, C. Wearables in Healthcare Organizations: Implications for Occupational Health, Organizational Performance, and Economic Outcomes. *Healthcare* **2025**, *13*, 2289. [\[CrossRef\]](#) [\[PubMed\]](#)
34. Mueller, W.; Smith, A.; Kuijpers, E.; Pronk, A.; Loh, M. Worker perspectives on improving occupational health and safety using wearable sensors: A cross-sectional survey. *Ann. Work. Expo. Health* **2024**, *68*, 867–873. [\[CrossRef\]](#) [\[PubMed\]](#)
35. Affia, A.O.; Finch, H.; Jung, W.; Samori, I.A.; Potter, L.; Palmer, X.-L. IoT Health Devices: Exploring Security Risks in the Connected Landscape. *IoT* **2023**, *4*, 150–182. [\[CrossRef\]](#)

36. Nithyavani, G.; Raja, G.N. A Comprehensive Survey on Security and Privacy Challenges in Internet of Medical Things Applications: Deep Learning and Machine Learning Solutions, Obstacles, and Future Directions. *IEEE Access* **2025**, *13*, 188955–188989. [[CrossRef](#)]
37. El Bouchikhi, M.; Weerts, S.; Clavien, C. Behind the good of digital tools for occupational safety and health: A scoping review of ethical issues surrounding the use of the internet of things. *Front. Public Health* **2024**, *12*, 1468646. [[CrossRef](#)] [[PubMed](#)]
38. Wang, M.; Sun, Y.; Sun, H.; Zhang, B. Security Issues on Industrial Internet of Things: Overview and Challenges. *Computers* **2023**, *12*, 256. [[CrossRef](#)]
39. Kaur, R.; Shahrestani, S.; Ruan, C. Security and Privacy of Wearable Wireless Sensors in Healthcare: A Systematic Review. *Comput. Netw. Commun.* **2024**, *2*, 27–52. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.