Computer Modeling in Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2024.053465

ARTICLE

IWTW: A Framework for IoWT Cyber Threat Analysis

GyuHyun Jeon[1], Hojun Jin[1], Ju Hyeon Lee[1], Seungho Jeon[2] and Jung Taek Seo[2,*]

[1]Department of Information Security, Gachon University, Seongnam, 13120, Republic of Korea

[2]Department of Computer Engineering (Smart Security), Gachon University, Seongnam, 13120, Republic of Korea

*Corresponding Author: Jung Taek Seo. Email: seojt@gachon.ac.kr

Received: 30 April 2024 Accepted: 20 August 2024 Published: 27 September 2024

ABSTRACT

The Internet of Wearable Things (IoWT) or Wearable Internet of Things (WIoT) is a new paradigm that combines IoT and wearable technology. Advances in IoT technology have enabled the miniaturization of sensors embedded in wearable devices and the ability to communicate data and access real-time information over low-power mobile networks. IoWT devices are highly interdependent with mobile devices. However, due to their limited processing power and bandwidth, IoWT devices are vulnerable to cyberattacks due to their low level of security. Threat modeling and frameworks for analyzing cyber threats against existing IoT or low-power protocols have been actively researched. The threat analysis framework used in existing studies was limited to specific protocols and did not target IoWT devices. In addition, In the literature surveyed to date, no cyber threat analysis framework is targeting IoWT. Therefore, the threat model presented in the existing research on cyber threat analysis and modeling for IoWT is specialized for specific devices. In addition, because it does not present standardized attack tactics and techniques, there is a limitation in that it is difficult to identify attacks quickly. In this paper, we propose an Internet of Wearable Things threat analysis frameWork (IWTW) framework that can derive security threats through systematic analysis of IoWT attack cases and possible security threats and perform cyber threat analysis based on them. The methodology for developing the IWTW framework consists of three steps: Analysis, Standardization, and Compilation. IoWT attack cases and potential security threats are analyzed in the analysis stage. In the standardization stage, attack tactics and techniques derived from the analysis of attack cases and potential security threats are standardized, resulting in 3 attack categories, 18 attack tactics, and 68 attack techniques. In the compilation stage, standardized security threats are combined to develop the IWTW framework ultimately. We present four case studies targeting MiBand 2, Fitbit Charge HR/Surge, Samsung Gear 3, Xiaomi Amazifit, Honor Band 5, Honor Watch ES, and Senbono CF-58 devices to validate the proposed IWTW framework. We analyzed the attack process through a case study and applied the IWTW framework to derive standardized attack categories, tactics, and techniques effectively. By applying the IWTW framework to cyber threat analysis targeting IoWT, security threats can be standardized, and the attack process can be quickly derived, enabling effective attack analysis on IoWT.

KEYWORDS

Internet of wearable things; wearable device; threat framework; security threat

Nomenclature

IoT	Internet of Things
IoWT	Internet of Wearable Things
BLE	Bluetooth Low Energy
LTE-M	Long Term Evolution for MTC
NB-IoT	Narrowband-IoT
NR-REDCAP	New Radio-Reduced Capability
NFC	Near-Field Communication
W2H	Wearables-to-Hub
W2I	Wearables-to-Infrastructure
W2W	Wearables-to-Wearables
GATT	Generic Attribute Profile

1 Introduction

The Internet of Wearable Things (IoWT) or Wearable Internet of Things (WIoT) is a new paradigm that combines IoT and wearable technologies. Advances in IoT technology have enabled the miniaturization of sensors embedded in wearable devices and the ability to communicate data and access real-time information over low-power mobile networks [1]. These advantages have led to a proliferation of personal wearable devices and the application of IoWT technology in various fields such as medicine, healthcare, and sports [2,3]. IoWT devices are interconnected by pairing with mobile devices to communicate with external servers to synchronize data, use web and phone services, and so on [4]. As such, mobile devices such as smartphones and tablets are highly interdependent as they serve as convenient gateways to IoT and wearable objects [5]. However, IoWT devices have difficulty using high computing security mechanisms such as Advanced Encryption Standard (AES), Rivest, Shamir, and Adleman (RSA) due to their limited processing power and bandwidth [6]. These characteristics make IoWT devices less secure than other devices, making them vulnerable to cyberattacks [7]. There are various attack methods against IoWT devices, including device disabling, unauthorized traffic access and analysis, and Man-in-The-Middle (MiTM) Attack.

There is an active research effort to analyze cyber threats targeting existing IoT or low-power protocols. Barua et al. [8] proposed the Bluetooth Low Energy (BLE) Threat Model, a comprehensive taxonomy of possible security and privacy threats to the BLE protocol, assuming it communicates with low-power, computationally constrained sensors and IoT devices rather than regular Bluetooth. They categorize security threats into eight categories based on the attacker's approach and the severity of the attack. Griffy-Brown et al. [9] proposed the Enterprise Risk Management Optimization (ERMO) framework, which describes cybersecurity in terms of risk for biodigital systems and represents a lifecycle approach to cyber risk management. The ERMO process consists of eight steps and includes two main goals: risk prioritization through risk analysis and organizational protection and evolution. It also provides a semi-quantitative method to score both risk and reward. The MITRE ATT&CK Framework is a security framework developed by MITRE Corporation that categorizes information about different attack techniques [10]. Based on actual cyber-attack cases, the attacker's behavior is categorized into various tactics and techniques. In addition, there are frameworks suitable for different network environments, such as Enterprise and Industrial Control System (ICS). Cybersecurity Competency for Research and Innovation (CMTMF) is a threat modeling framework for mobile systems created by the Cyber security cOmpeteNC fOr Research anD InnovAtion (CONCORDIA) project

to highlight the importance of cyber threat intelligence skills [11]. The Wearable Smart Health Device (WSHD) Threat Model examines exploitable aspects of wearable smart health devices, such as sensors connected to the Internet, to monitor the wearer's health and exchange data [12]. The threat model targets the WSHD device-companion app and companion app-cloud communication sections and includes security threats that may occur in WSHD communication. The MEDICALHARM is a threat modeling methodology tailored to identify threats in Modern Medical Devices (MMD) systems [13]. The proposed methodology combines security threats and risk analysis.

However, the following problems exist with IoWT in existing research. Since the threat model is limited to BLE, applying it to security threats in other wireless communication protocols is difficult. The ERMO model is too comprehensive a concept to derive attack tactics and techniques, so it is difficult to classify cyber threats properly. CMTMF is divided into 105 attack actions and 14 tactical categories, but unlike MITER ATT&CK, there are no unique tactics. The WSHD Threat Model did not standardize security threats' attack tactics and techniques. This renders it impossible to define the scope and characteristics of security threats properly and causes low accuracy in attack identification. The MEDICALHARM has a total of 11 distinguishable attack tactics and techniques, which is very small. Additionally, the selected security threats have inaccurate attack tactics and techniques. For this reason, a cyber threat analysis framework that is specialized for IoWT and can standardize various attack tactics and techniques is needed. Therefore, the low power and communication protocol characteristics of IoWT devices must be considered. Additionally, reliable classification criteria must be selected to identify attack tactics and techniques in IoWT security threats accurately.

In this paper, we propose the Internet of Wearable Things threat analysis frameWork (IWTW) framework, which derives security threats through systematic analysis of IoWT attack cases and possible security threats and performs cyber threat analysis based on them. The methodology for developing the IWTW framework consists of three stages: Analysis, Standardization, and Compilation. In the Analysis phase, we analyze the attack cases performed against IoWT devices and derive the attack process and security threats. It includes the IoWT Attack Cases course, which analyzes possible attack cases against IoWT, and the IoWT Security Threat course, which analyzes potential security threats that may occur in IoWT. In the Standardization step, the data derived from the analysis of attack cases and potential security threats is organized into 3 attack categories, 18 attack tactics, and 68 attack techniques. The IWTW framework is developed in the Compilation step by combining the security threats organized in the previous step. The IWTW framework comprises 18 standardized attack tactics and 68 detailed attack techniques based on three attack categories: Launch on Attack, Expand Attack, and Attack Result. We applied case studies on MiBand 2, Fitbit Charge HR/Surge, Samsung Gear 3, Xiaomi Amazifit, Honor Band 5, Honor Watch ES, and Senbono CF-58 devices to validate the proposed IWTW framework. Afterward, the evaluation results are compared with existing studies, and study limitations are discussed.

The primary contributions of this paper are as follows:

- We propose a methodology and the IWTW framework based on IoWT attack cases and possible security threats to analyze cyber threats against IoWTs. Through the IWTW framework, security threats can be classified into 3 attack categories, 18 attack tactics, and 68 attack techniques.
- The proposed framework accurately defines the scope and characteristics of attacks by standardizing various attack tactics and techniques used in security threats occurring in the IoWT environment, leading to more accurate attack identification.

- We validated the IWTW framework through case studies that performed attacks targeting actual IoWT devices and derived the strengths and weaknesses of our framework.

This paper is organized as follows. Section 2 provides an overview of IoWT, IoWT network structure, and differences between IoWT and IT networks. Section 3 analyzes existing research related to cyber threat analysis and frameworks for IoWT. Section 4 presents the methodology and IWTW framework we developed for analyzing cyber threats targeting IoWT. Section 5 presents a case study of the IWTW framework. Section 6 provides a discussion of this study. Section 7 presents conclusions and future work.

2 Background

Section 2 reviews the literature on IoWT overview and reference architecture, possible security threats to IoWT devices, and existing threat modeling frameworks.

Fig. 1 provides an overview of wearable devices' typical components and communication processes [14–16]. The wearable device's sensors, such as accelerometer, gyroscope, and magnetometer, allow you to input data or monitor your activity. Then, it connects with the mobile device by performing a pairing process such as Bluetooth's Generic Attribute Profile (GATT) and Generic Access Profile (GAP). After that, the information from the mobile device, such as a smartphone, is transmitted to the server or Personal Computer (PC) via wireless communication. Finally, the processed data is returned to the paired wearable device or smartphone. The wearable device can directly connect with the mobile device or PC via Wi-Fi (WLAN) based on the wireless module.

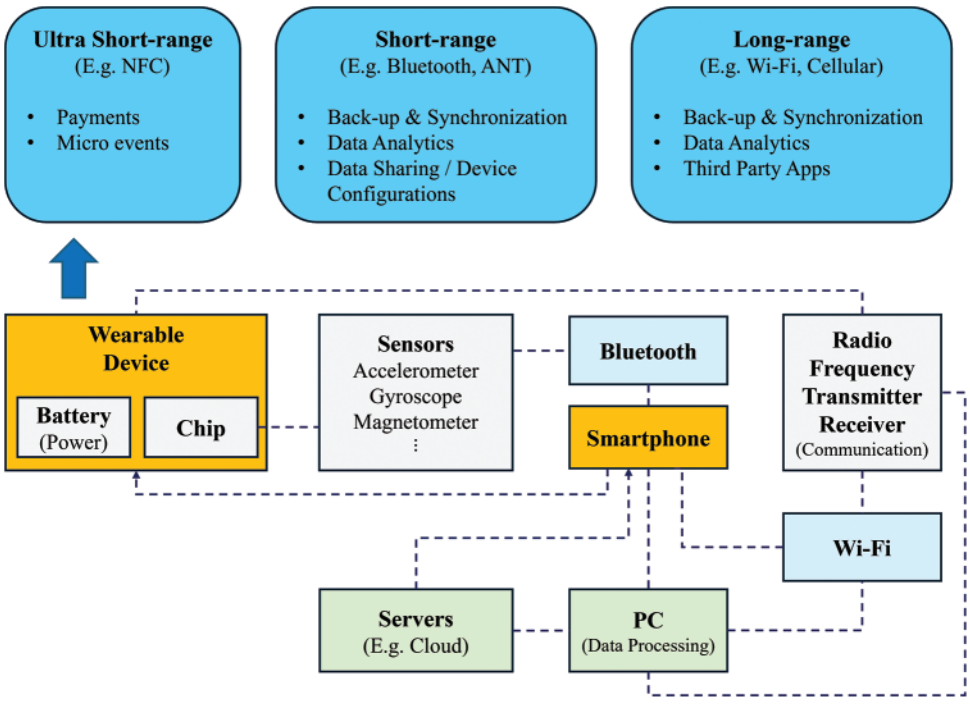

Figure 1: Overview of wearable device structure and communication

Meanwhile, wearable devices support different communication ranges. They use various wireless communication protocols such as Near Field Communication (NFC), Wi-Fi, Bluetooth Security measures for wireless data access are essential as they often involve transmitting personal information, such as financial payments, healthcare. However, resource constraints in the form of limited battery, CPU, memory, and device form factors of wearable devices limit the implementation of high-level security mechanisms.

IoWT network topologies are generally classified into three categories based on the network connection structure. Table 1 provides information on the technologies typically used for wireless communication in IoWT devices, categorized by interaction method, connection time, and data processing speed. IoWT network topologies are generally categorized into three types based on the network connectivity structure.

Table 1: IoWT wireless communication technology

Ref.	Connection technology	Interconnection method	Connection distance	Data transfer speed
[17]	Wi-Fi direct	W2H, W2I, W2W	$\leq$ 200 m	$\leq$ 250 Mbps
[18]	BLE	W2H, W2W	$\leq$ 300 m	$\leq$ 50 Mbps
[19]	NFC	W2H	$\leq$ 0.2 m	$\leq$ 424 kbps
[20]	Zigbee	W2H, W2W	$\leq$ 100 m	$\leq$ 250 kbps
[21]	LTE-M	W2I	$\leq$ 10 km	$\leq$ 1 Mbps
[21]	NB-IoT	W2I	$\leq$ 15 m	$\leq$ 250 kbps
[22]	NR-REDCAP	W2I	$\leq$ 10 km	$\leq$ 150 Mbps

Wearable to Hub (W2H): Interconnected with a hub, such as a smartphone, PC, or tablet. The purpose is to collect data from IoWT devices and connect them to the external Internet. The hub requires high computing capacity to process the data, including storing and distributing the collected data. It also requires at least two interfaces for data collection and internet connection [16].

Wearble to Infrastructure (W2I): IoWT devices are directly interconnected to network base stations such as NodeB/eNodeB/gNodeB, or to the Internet such as 3G/4G/5G, Wi-Fi, and each device includes Wi-Fi or cellular connectivity. For example, applications on smartwatches process data sensed by IoWT devices locally and then interact directly with central servers on the Internet [23].

Wearable to Wearable (W2W): This is the interconnection between wearable devices. It aims to communicate directly between IoWT devices to exchange information. It has good dash time and responsiveness in communication, but it has limitations in resource capacity due to the nature of connecting wearable devices [10,24].

Table 2 summarizes the differences between IT and wearable networks [25–30]. The differences between IT and wearable network communications are as follows: IT networks vary in size depending on whether they are home or business networks and consist of computers, servers, and other interconnected devices to send and receive data and resources [31]. Wearable networks, on the other hand, include wearable devices such as smartwatches, smart glasses, smart bands, and fitness trackers and are smaller than IT networks because they are primarily human-centric connections that monitor the user's physical condition [1,25,26]. Wearable devices also prioritize low power consumption due to battery size constraints, so they often use protocols such as BLE, which are designed to minimize

power usage during the communication process [27]. Wearable communications also connect with mobile devices to improve processing performance, as they operate over shorter distances than typical IT communications and have slower data processing speeds due to the miniaturization of the devices [25,28–30]. Wearable devices used for health or medical purposes send and receive sensitive data, such as bodily information, making security for wearable networks important [25].

Table 2: Summary of differences between IT and wearable network communications

Difference	IT network	Wearable network
Network size	• Various	• Usually small (e.g., Personal area network (PAN))
Network performance	• High	• Low
Power consumption	• High	• Low
Data processing speed	• Very fast	• Slow
Connection distance	• Very long	• Short
Transmission and reception data	• Various	• Limited

3 Related Works

Section 3 reviews the research related to cyber threat analysis and frameworks for IoWT.

A cyber threat analysis framework is a systematic approach to quickly identifying and managing security threats to a system from external cyberattacks. It is necessary to analyze attack vectors, design defensive techniques against security threats, and implement countermeasures and follow-up actions.

As shown in Table 3, Sections 3.1 and 3.2 categorize existing research according to the target of threat modeling. Afterwards, we provide examples of cyber threat analysis frameworks and model studies related to medical devices and IoT, including the BLE Threat Model, ERMO, MITRE ATT&CK, CONCORDIA–CMTMF, Emerging Miniaturized Wireless Biomedical Devices (MWBD), Bhadra, WSHD Threat Model, and MEDICALHARM.

Table 3: Related literature

Ref.	Main idea	Framework/model name	Advantage	Disadvantage
[8]	• Categorizes security threats targeting low-power BLE	BLE threat model	• Attack techniques and detailed technical representations	• Limited to BLE only
[9]	• Provides a foundation and methodology for analyzing cyber-biological risks	ERMO	• Identify security threats to categorize attack vectors	• Too comprehensive methodology

(Continued)

Table 3 (continued)

Ref.	Main idea	Framework/model name	Advantage	Disadvantage
[10]	• Categorizes attacker behavior into different tactics and techniques based on real-world cyberattack cases	MITRE ATT&CK	• Systematic approach categorized by attack tactics and techniques	• Does not consider IoWT
[11]	• Threat modeling framework for mobile systems	CONCORDIA–CMTMF	• Systematic approach in mobile systems	• Does not consider IoWT
[12]	• Threat modeling for WSHD devices	WSHD threat model	• Identify vulnerabilities in WSHD devices	• Unstandardized attack tactics and techniques
[13]	• Threat modeling methodology for MMDs	MEDICALHARM	• Systematic approach in medical devices	• Few classifiable attack tactics and techniques
[32]	• Propose threat modeling for mobile healthcare devices	Emerging MWBD	• Security threat identification and risk management	• Too comprehensive modeling
[33]	• Threat modeling framework for mobile networks	Bhadra	• Systematic approach in mobile networks	• Does not consider IoWT

3.1 IT, IoT, and Mobile Threat Model & Framework

The ERMO framework [9] describes cybersecurity in terms of risk for biodigital systems and points to a lifecycle approach for cyber risk management. Since biodigital systems encompass both life sciences and cybersecurity, risk analysis through this framework includes digital, hardware, and biological assets. Risk in the ERMO process includes two main goals: prioritizing risks through analysis, protecting and evolving the organization, and providing a semi-quantitative way to score both risk and reward. It also provides an initial identification of key exposure variables and loss drivers for biodigital systems. The ERMO Framework's methodology consists of eight steps. Steps 1 and 2 prioritize risks, including cyberbio assets, operations, and liabilities. Step 3 identifies the causes of loss or risk that impact Steps 1 and 2. Step 4 is the consequences of the impacted risks. Step 5 includes controls to minimize loss frequency and/or severity. Steps 6 and 7 assess the damage to components, such as cyberbio systems, subsystems. Step 8 includes implementing and monitoring risk controls and risk financing plans and programs. Based on the proposed methodology, key exposures, exposure variables, and sources of loss can be identified and developed into a risk registry. However, the ERMO model is too broad to categorize the tactics and techniques used against cyber threats properly. Since the threat model does not classify detailed attack tactics and techniques, in-depth cyber-attack analysis is difficult. The study did not include specific attack tactics and techniques to classify. In addition, the proposed framework does not have a validation process, and thus its reliability is low.

The MITRE ATT&CK Framework [10] is a security framework developed by MITRE Corporation that categorizes information about different attack techniques. The attacker's behavior is categorized into different tactics and techniques based on actual cyber-attack cases. This framework is used to analyze attack patterns and derive attack behaviors to improve the ability to detect advanced attacks. The MITRE ATT&CK database contains useful information on threat modeling languages, such as assets (e.g., computers, services, internal and external networks), attack phases (e.g., spearphishing attachments, user execution), and threat modeling languages. The data can be used to develop various threat models and methodologies. Some frameworks, such as Enterprise and ICS, are appropriate for different network environments. However, the MITER ATT&CK Framework does not specialize in IoWT. Because IoWT devices operate in a unique environment due to limitations such as low processing power and bandwidth, applying all attack techniques proposed in existing IT and ICS frameworks is difficult.

CMTMF [11] is a threat modeling framework for mobile systems created by the CONCORDIA project to highlight the importance of cyber threat intelligence techniques. This study focusing on threats to the mobile network itself, the entry points for carrying out attacks were analyzed as follows: the mobile device, the SIM Card, the mobile app, the gNodeB, the IPUPS, the SEPP, and the Network Exposure Function (NEF)-CAPIF. It was developed to address the difficulties in applying existing threat modeling frameworks such as MITRE ATT&CK and Bhadra framework to mobile networks. CMTMF is compatible with sub-frameworks of MITRE ATT&CK, such as MITRE ATT&CK for Enterprise, Mobile, and ICS. CMTMF is divided into 105 attack behaviors and 14 tactic categories, but unlike MITRE ATT&CK, there are no unique tactics. Instead, the attacks are characterized by the use of multiple devices on a mobile network and the repetitive nature of the attacks, so the attacks are documented in a step-by-step loop. However, it does not consider the wearable environment. IoWT devices perform special network communications such as BLE, NFC, and Zigbee and operate in the unique environment of wearables. This indicates that existing IT and ICS target threat analysis techniques cannot be applied accurately.

MWBDs [32] are miniaturized mobile healthcare devices used in healthcare services such as telemedicine and have limited resources (size, power, processing, and storage). Due to these characteristics, they pose security risks to the privacy of users while collecting and transmitting patients' sensitive personal information. Therefore, this study proposed a methodology to counter cyberattacks on MWBDs. In MWBD, threat modeling, assets, vulnerabilities, threats, attacks, risk classification, and risk assessment are performed. First, assemble a team to perform threat modeling. The threat modeling team should include at least one member from each engineering group involved in hardware, radio links, and software to ensure a solid understanding of the underlying technology. Next, the security assumptions and constraints against which the threat modeling is performed to capture information at the appropriate level of abstraction are identified. The operating environment is analyzed during this process, and security domains/perimeters/use cases are defined. Later, attackers are defined, followed by a systematic analysis of security threats. Finally, once the risks to the system are defined, risk management is performed to assess, monitor, and respond to the risks. This study validated the proposed MWBD threat modeling by conducting a case study on MWBD devices with the following characteristics: Injectable, Ingestible, Implantable, and Wearable. However, this threat modeling methodology is too broad a concept for detailed threat analysis. The proposed threat model did not provide detailed information about attack tactics and techniques to classify cyberattacks in detail. For example, no specific classification has been performed on attacks that occurred during the BLE pairing process between a wireless implantable neural interface system on a chip (SoC) and an external terminal.

The Bhadra framework [33] is a threat modeling framework that classifies publicly known security threats to mobile networks into nine tactical and 55 technical categories. It focuses on 2G, 3G, and 4G technologies based on 3GPP standards. The BHADRA framework identifies a wide range of potential attackers by modeling even attacks that have not been observed in practice. The threat modeling methodology consists of three phases, and the attack lifecycle proceeds in the following order: attack mounting, attack execution, and attack consequences. Attack mounting is when an attacker finds a target's weaknesses, gains initial access to the target, and establishes a persistent presence. Attack execution is where the attacker exploits vulnerabilities in the system to extend control from initial access to the target. Attack results are when the attacker achieves their tactical objectives, primarily related to information gathering and other attack impacts. However, the proposed Bhadra framework has limitations when applied to IoWT. For example, Attack Progression's SS7-based techniques include protocols such as the Signaling Connection Control Part (SCCP) and Transaction Capabilities Application Part (TCAP). Security threats cannot be identified since IoWT devices do not support these protocols.

3.2 IoWT Threat Model & Framework

The BLE Threat Model [8] represents a comprehensive categorization of security and privacy threats to the BLE protocol, which is based on communicating with low-power, computationally limited sensors and IoT devices rather than regular Bluetooth. First, we categorize the security threats into eight categories based on the attacker's approach and the severity of the attack. Attacks that perform similar attack techniques are combined into one category. The security threats are classified as follows: Passive Eavesdropping, which occur due to the simplified and predictable design of BLE channel hopping; Active Eavesdropping, where an attacker positions itself in the BLE communication path to steal information; and Device Cloning, where an attacker causes damage by pretending to be a trusted device of the target, cryptographic vulnerability, which exploits cryptographic weaknesses and flaws in the BLE protocol; DoS, which occurs at the physical and network layers to prevent the intended user from using system resources; Distortion, which attacks the services of a BLE device by exploiting vulnerabilities in BLE protocol services and BLE data packets; and Surveillance, which is used to identify BLE devices. However, since the BLE threat model targets only a single protocol, it is unsuitable for security threats to various protocols used in IoWT. Many communication protocols are used between wearable devices and mobile devices, such as NFC, Zigbee, Wi-Fi Direct, and NB-IoT. Therefore, it must be possible to target multiple protocols.

The WSHD Threat Model [12] examines exploitable aspects of wearable smart health devices, such as sensors connected to the Internet, to monitor the wearer's health and exchange data. The proposed threat model represents the companion apps, cloud, and communication protocols of the WSHD system. The threat model targets the following two communication sections, which include security threats that may occur in communications established in the WSHD system: WSHD device-companion app and companion app-cloud. This study selected Garmin Connect, Polar Beat, Mysugr, and Finger Oximeter-SpO2 companion apps to verify the proposed threat model and analyze their vulnerabilities. The programs and tools used are Wireshark, BLECryptracer, and Logcat. The security threats identified include network packet sniffing, traffic capture and manipulation, data collection using valid APIs, and encryption vulnerabilities. However, a formalization process was not performed on the attack tactics and techniques used in security threats. If there is no formalization process for attacks, the scope and characteristics of security threats cannot be properly defined, which reduces the accuracy of attack identification.

The MEDICALHARM [13] is a threat modeling methodology tailored to identify threats in MMD systems. The proposed methodology combines security threats and risk analysis. The primary security threats are security and privacy threats and include Modification breach, Exposure of sensitive or personal data, Denial of service, Impact of threat, Component threat, Access breach, Likelihood of threat, Harm to the patient, Assumptions and constraints about the system, Relevant in-depth threat, Monitoring and logging. The risk analysis adopts the semi-quantitative analysis recommended by the National Institute of Standards and Technology (NIST). This study uses CVSS scores to assess the risk of all identified vulnerabilities, combined with qualitative likelihood and impact measures. However, the proposed threat modeling has few distinguishable attack tactics and techniques, totaling 11. In addition, the selected security threats are not at the same level, so the scope of analysis is different. For example, Denial of service is included in the attack technique, but the Component threat is included in the attack tactic. Therefore, the number of attack tactics and techniques that can actually be classified is smaller.

4 Framework for IoWT Cyber Threat Analysis

Section 4 introduces IWTW, a cyber threat analysis framework. Existing cyber threat analysis frameworks are not specialized for IoWT environments, which makes it difficult to analyze attacks. Therefore, we propose IWTW, a framework for analyzing cyber threats targeting IoWT. Section 4 consists of the development methodology, the analysis of IoWT attack cases, the formalization of attack tactics and techniques in threat data, and a detailed description of the developed IWTW framework. Most attack tactical categories applied in the IWTW framework are based on the MITRE ATT&CK framework. However, MITRE ATT&CK does not cover frameworks based on IoT or IoWT systems, so it cannot properly evaluate IoWT attacks. Therefore, the IWTW Framework modifies existing attack tactics and techniques or adds new attack tactics to fit the IoWT environment. The IWTW Framework may be regularly updated with data on attack tactics and techniques in the future.

4.1 Methodology for Developing IWTW Framework

Section 4.1 describes the IWTW cyber threat analysis framework. IoWT attack cases, IoWT security threats, and attack tactics and techniques were derived from a variety of literature, including technical reports, white papers, studies, and academic publications. The methodology is divided into three phases. Fig. 2 shows an overview of the IWTW framework development methodology.

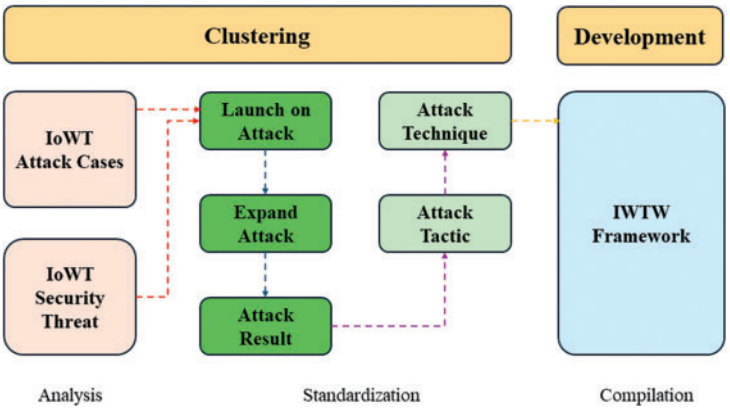

Figure 2: Methodology for developing IWTW framework

Step 1 Analysis: Analyze the attack cases and derive the attack process performed against IoWT devices.

Step 2 Standardization: Standardize attack tactics and techniques derived from the analysis of attack cases and potential security threats.

Step 3 Compilation: Combining the security threats formalized in the previous step to propose an IWTW framework.

The proposed methodology is divided into two areas: Clustering and Development. First, the Clustering area stores data derived from the analysis of attack cases targeting IoWT and potential security threats that may occur in IoWT. The clustering area requires continuous updates in response to new cyber-attacks. In addition, it consists of two parts: Analysis and Standardization. First, the Analysis part includes IoWT Attack Cases, which analyzes attack cases that can occur against IoWT, and IoWT Security Threat, which analyzes potential security threats that can occur in IoWT. IoWT Attack Cases is based on actual attacks against IoWT and analyzes the attack process and security threats. IoWT Security Threat is not derived from the attack cases that were previously analyzed, but it analyzes the security threats that can be caused by potential attackers targeting IoWT. The Standardization part performs the process of standardizing the attack categories, attack tactics, and attack techniques derived from the Analysis part.

The equation for the proposed methodology is as follows: The set of security threats derived through IoWT Attack Case and IoWT Security Threat are X and Y. IoWT attack data is collected as much as i. Z means set in which duplicates of the derived security threats have been removed. The set Z is defined as follows: $Z = \bigcup_{i=1}^{n}(X_i \cup Y_i)$. Attack categories are defined as follows: Launch on Attack, Expand Attack, and Attack Result are expressed as a_1, a_2, a_3. The elements z_k of set Z can be classified into a_i. The relationship between z_k and a_i is defined as follows: $\forall z_k \in Z, \exists a_i \in \{a_1, a_2, a_3\}$: $z_k \in a_i$. Attack tactics classified within attack category a_i are b_1 to b_n. Attack Techniques classified within attack tactics b_j are c_1 to c_n. a_i contains attack tactics b_j, and b_j contains attack techniques c_k. The relational expressions for a_i, b_j, and c_k are defined as follows: $\forall a_i \exists b_1, \ldots, b_n \subseteq a_i$: $\forall b_j, \exists c_1, \ldots, c_n \subseteq b_j$

In the development area, a cyber threat analysis framework for IoWT is developed based on threat analysis data from the clustering area. By combining the standardized attack categories, attack tactics, and attack techniques, the IWTW framework is finally developed.

4.2 Step 1: Analyze IoWT Attack Cases and Possible IoWT Security Threats

Section 4.2 reviews IoWT attack cases and analyzes potential IoWT security threats.

4.2.1 IoWT Attack Cases

IoWT devices typically collect data and process important information from clients. Popular types of IoWT devices include NFC Smart Ring, Smart Posture Trainer, Gaming Simulator, Smart Shoes, Smart Jewelry, Fitness Tracker, Smart Band for Blinds, Smart Clothing, GPS Tracking Band [19,20]. Table 4 analyzes the attack cases against these IoWT assets. The attacks are categorized into IoWT assets, attack processes, and threat techniques based on the targets and attack methods.

Table 4: Cases of cyber-attack targeting IoWT device

Ref.	IoWT asset	Attack process	Security threats
[8]	Smart watch	• Through the GATT protocol, neighboring wearable devices broadcast a signal, and the master (Mobile) connects to the signal. • Exploit a vulnerability in the internal mechanism of the GATT protocol where services can be easily cloned and spoofed. • The attacker uses a fake mobile app to impersonate a BLE wearable device, and the master connects to the malicious device. • The malicious device propagates the connection with the original device and performs an ITM attack.	• Man-in-the-middle attack, protocol vulnerability, eavesdropping
[34]	Smart watch	• Use the Bluefruit LE sniffer tool to capture BLE traffic. • Analyze the data packets using wireshark, an open-source packet analyzer. • Identify smart wearable device type and version via static addresses in the analyzed packet data.	• Passive sniffing attack, traffic capture
[35]	Smart band	• Normal use between wearable devices and mobile (gateway). • The cracked app is installed on the attacker's smartphone. • Forced pairing between wearable device and attacker smartphone via cracked app. • Exploitation of a vulnerability where the wearable device and smartphone do not authenticate each other every time they connect, preventing the wearable device from distinguishing between the real user's smartphone and the attacker's smartphone.	• Malicious app, illegal device pairing, absence of certification

(Continued)

Table 4 (continued)

Ref.	IoWT asset	Attack process	Security threats
		• Collecting health data from the wearable device, such as the user's heart rate, physical activity, and calorie consumption. • The collected data is sent to the attacker's smartphone.	
[36]	Smart band	• Detect smart band devices using vulnerability scanning tools. • Eavesdropping the BLE protocol. • Using the Adafruit BLE sniffer nRF51822 in an Ubuntu virtual machine on VMWare to sniff packets exchanged during BLE communication. • Performed healthcare-related data exfiltration and packet injection, including user steps, distance traveled, calories burned.	• Scanning, sniffing, data extraction, packet injection
[37]	Smart watch	• Performing active scanning utilizing the Nmap security scanner tool modified to run in an android wear environment. • A ZGPAX S8 smartwatch/phone device runs a malicious access point using the same SSID name as an HP OfficeJet 8610 Wi-Fi direct printer. • Selecting and connecting to a fake Wi-Fi direct printer based on its SSID name when a victim attempts to send a print job from their laptop. • Sending a printout containing sensitive data to the attacker in a file format such as PDF.	• Scanning, malicious app, eavesdroppinl

(Continued)

Table 4 (continued)

Ref.	IoWT asset	Attack process	Security threats
[38]	Fitness tracker	• Tracking the victim using a vulnerability in the Fitbit tracker that always uses the same device address. • Connect to a Fitbit tracker paired to a mobile device using the GattTool utility. • Automated shell script that continuously reads the tracker's characteristics and causes it to respond to all requests (DoS attack, reducing availability).	• Same device address, protocol vulnerability, vulnerability tool, automated shell script, DoS, preventing service
[39]	Fitness tracker	• Blocks multiple services, including phone, increasing battery utilization and causing pairing blocking. • The microprocessor does not have the necessary protection to lock out external reads and writes to internal flash, targets Nike+Fuelband devices with USB connectors. • Uses standard ST microelectronic development tools to communicate with the STM32 system and obtain the device's firmware.	• USB connect, corrupted firmware, string replacement

(Continued)

Table 4 (continued)

Ref.	IoWT asset	Attack process	Security threats
[40]	Fitness tracker, smart watch	• Apply the modified firmware via the USB connector to perform the attack (change strings). • Ubertooth one is a BLE antenna that provides spectrum analysis (similar to sniffing) of the 2.4 GHz radio band in a simple plug-and-play USB dongle. • Targets Jawbone UP, pebble steel, and Fitbit charge HR wearables. • Enable Ubertooth on the attack system using the command ubertooth-btle-fc/tmp/pipe. • Activate mobile's bluetooth feature to pair the phone to the device using the specific pairing process for each wearable device. • Ubertooth is actually responsible for sending data from the wearable to the vendor-specific app on the phone, while Ubertooth continues to sniff and capture the packets going back and forth.	• Protocol vulnerability, USB connect, sniffing, data extraction, MITM attack

4.2.2 IoWT Security Threat

In addition to the examples of IoWT attacks analyzed in Section 4.2.1, we also considered IoWT attacks that potential attackers or security threats could cause. Table 5 shows the potential security threats and their descriptions for IoWT, derived from a literature review of papers, studies, and technical reports related to cybersecurity threats to IoWT. The possible security threats were analyzed by considering confidentiality, integrity, and availability issues for IoWT [41,42]. Confidentiality breaches include unauthorized access to resources by unauthorized users, and related security threats include access to user information, such as accessing and analyzing communication traffic between wearable devices, eavesdropping, and information-gathering attacks. Integrity breaches involve modifying sensitive information collected from wearable devices, such as user physical and medical information, and related security threats include reply, modification, and masquerade attacks on wireless communications. Availability breaches involve causing a wearable device to behave erratically or block communication, and related security threats include denial-of-service attacks.

Table 5: Potential security threats targeting IoWT device

Ref.	Security threat	Description
[43]	Active sniffing	• An attacker impersonates a legitimate device or actively manipulates connection parameters.
[44]	Authentication bypass	• Successful exploitation of this vulnerability will cause the access control functionality of certain applications to fail. • (e.g., Huawei children smart watch (Simba-AL00) 1.1.1.274).
[45]	Automated shell script	• Mimics a DoS attack to initiate a connection request and read the characteristics of the wearable device.
[46]	Bluebugging	• Allow an attacker to take control of a Bluetooth-enabled device without the user's knowledge. Exploit vulnerabilities in the Bluetooth protocol or device firmware to remotely execute commands.
[47]	Command injection	• An attack that aims to execute arbitrary commands on the host operating system through a vulnerable application.
[48]	Data extraction	• Used by attackers to steal data from the network.
[49]	Denial of service	• Sends many requests to the target device in a short time or sends requests to the target device that it does not know how to process.
[50]	Firmware access	• Successful access to firmware, which can lead to future updates and increased privileges for the attacker.
[51]	Firmware corruption	• The attacker manipulates, overwrites, or corrupts the firmware to deny use of the system or device.
[52]	Fixed device address	• Random address programmed or generated by the device at runtime on a BLE device.
[53]	Illegal device pairing	• The attacker attempts to connect to a BLE-enabled device without user knowledge or consent.
[54]	Illegal filming	• Abuse the recording capabilities of smart glasses to illegally take photos and videos.
[55]	Information gathering	• Gather information about wearable devices and use the information to analyze the vulnerabilities of the device and increase the number of possible ways to attack it.
[56]	Leaky BTLE	• The number of TKs that can be used to generate STK in the STK generation stage is small.
[57]	Location tracking	• Leveraging BLE used in wearable devices to track users by intercepting and analyzing signals emitted for legitimate functions such as device location services.
[58]	Malicious app	• Malicious apps are installed on mobile devices and forced to connect with wearable devices, compromising data security.

(Continued)

Table 5 (continued)

Ref.	Security threat	Description
[59]	Malware attack	• Malware is installed on a mobile device and forced to connect with a wearable device, compromising the wearable device's sensors.
[60]	Masquerade attack	• The attacker impersonates a legitimate IoWT device or user to gain unauthorized access or manipulate the system.
[61]	MITM attack	• Occurs when an attacker intercepts and alters communications between two parties, acting as an unwitting intermediary. Used to intercept authentication credentials, session keys, or other sensitive data exchanged during the pairing process.
[62]	Modification attack	• Since data transfer between wearable devices is performed over the air, an attacker can intercept the wearable device's traffic exchange or modify the contents of the exchange packets after gaining access to the information.
[63]	Non-authentication	• Wearable devices lack authentication mechanisms.
[64]	Non-encrypted data	• Poor implementation of encryption in communication protocols used in wearable devices
[65]	Packet injection	• Intentionally sending altered or manipulated data packets to manipulate or disrupt the normal operation of the wearable device.
[66]	Passive sniffing	• The attacker passively intercepts communications without actively participating in the connection. Use of specialized hardware or software tools that can capture packets.
[67]	Physical access	• Physically accessing the wearable device, such as via USB, to perform physical compromise and spoofing attacks.
[68]	Replay attack	• An attacker captures packets and retransmits them to the target for malicious purposes.
[69]	Service stop	• The attacker stops or disables services on the system so that legitimate users cannot use those services.
[70]	Third-party	• Passing key information such as personal information and wearable device key information to third parties, but the data is stored in plain text and is vulnerable.
[71]	Traffic analysis	• Analyze communication traffic from captured wearable devices to gain access to sensitive data, such as user activity in network traffic.

(Continued)

Table 5 (continued)

Ref.	Security threat	Description
[72]	Traffic capture	• A tool like pcap can be used to capture communication traffic from a wearable device.
[73]	Unauthorized access	• Gain unauthorized access to the wearable device or network to prepare for further attacks.
[74]	Unsecure network	• Data is transmitted over an unsecured network or in an unencrypted format.
[75]	Unsecure PIN	• Lack of authentication due to unsecured PIN systems within the wearable device.
[76]	Vulnerable protocol	• Security vulnerabilities in communication protocols between wearable devices, such as MQTT, BLE.
[77]	Weaponization	• Attacking a wearable device, such as a wearable medical device, and then manipulating it to perform malicious behavior causing actual damage.
[78]	Wireless access	• Communication methods based on wireless LAN standards such as Wi-Fi Direct and BLE. Wearable devices connected to these wireless access points can be attacked.

4.3 Step 2: Standardization of Attack Tactics and Techniques

In this session, we will formalize the attack tactics and techniques derived from our analysis of attack cases and potential security threats against IoWT devices in Section 3.2. Attack categories represent the initiation, progression, and consequence phases of an attack. Attack tactics represent the attacker's behavior in accordance with the attack goal. Attack techniques represent how the attacker achieves the attack tactic against the goal, and there are various attack techniques for each attack tactic. This study referenced the MITRE ATT&CK Framework to formalize attack tactics and attack techniques but did not include them in the formalization process if they are not applicable or not applicable to IoWT devices.

4.3.1 Launch on Attack

Launch on Attack is categorized into three attack tactics: Reconnaissance, Resource Development, and Initial Access. It represents a possible security threat in the early stages of an attack, such as when an attacker discovers a security weakness in a target. The attack can be expanded based on the information gained during this phase.

Reconnaissance is an attack tactic that gathers information that can be used in an attack. It includes the Exploitation of Wireless Device Configuration, Active Scanning, and Passive Scanning attack techniques. Table 6 shows the attack techniques used in the Reconnaissance tactic and their descriptions.

Table 6: Attack techniques and detailed descriptions used in Reconnaissance

Attack tactics	Ref.	Attack techniques	Description
Reconnaissance	[79]	Exploitation of wireless device configuration	• It filters and analyzes wireless network traffic to leverage specific components such as source and destination addresses, protocols used, and data payloads.
	[80]	Active scanning	• Unlike other forms of reconnaissance that do not involve direct interaction, scanning attacks involve the attacker probing the victim's infrastructure through network traffic.
	[81]	Passive scanning	• In a scanning attack, the attacker sends standard communication messages to the target's wearable device and gathers the necessary public information from the returned response messages.

Resource Development is an attack tactic in which an attacker creates, purchases, compromises, or steals resources such as tools or vulnerabilities that can be used in an attack, and includes the Obtain Capabilities, Develop Capabilities, and Stage Capabilities attack techniques. Table 7 shows the attack techniques used in the Reconnaissance attack tactic and their detailed descriptions.

Table 7: Attack techniques and detailed descriptions used in resource development

Attack tactics	Ref.	Attack techniques	Description
Resource development	[82]	Obtain capabilities	• The attacker obtains information about software tools or vulnerabilities needed for the attack (e.g., purchased, downloaded, stolen).
	[83]	Develop capabilities	• The attacker builds the software tools needed for the attack or discovers vulnerabilities.
	[84]	Stage capabilities	• The attacker deploys the capabilities required for the attack into the target's network infrastructure.

Initial Access is an attack tactic for attack vectors used to gain an initial foothold within a mobile or wearable device network. It includes the Exploit Public-Facing Application, Deliver Malicious

App, Network Configuration Manipulation, and Replication Through Removable Media attack techniques. Table 8 shows the attack techniques used in the Initial Access attack tactic and their detailed descriptions.

Table 8: Attack techniques and detailed descriptions used in initial access

Attack tactics	Ref.	Attack techniques	Description
Initial access	[85]	Exploit public-facing application	• An attacker attempts to exploit a weakness in a host or system connected to the internet to gain initial access to a network. This includes vulnerabilities in communication protocols (e.g., GATT) and applications for wearable devices.
	[86]	Deliver malicious app	• Malicious or cracked applications are installed on a wearable or mobile device through legitimate channels.
	[87]	Network configuration manipulation	• An attacker can manipulate the configuration of a network to run a malicious access point by manipulating the SSID name of a malicious wearable device to be the same SSID as the target's Wi-Fi direct printer.
	[88]	Replication through removable media	• The attacker exploits or copies malicious code onto a device connected via USB and moves it to the wearable device. The attacker can then attempt to exploit the device by accessing stored data.

4.3.2 Expand Attack

The Expand Attack phase extends the attack process to the attacker's intended goal through various methods, including vulnerability exploitation, after successful initial access to the target. Expand Attack is categorized into nine attack tactics: Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, and Command and Control.

Execution is an attack tactic that involves executing code and files to control a wearable device and includes the Application Layer Protocol, Native API, Command and Scripting Interpreter, Device

Synchronization, and Firmware Update attack techniques. Table 9 shows the attack techniques used in executing the attack tactics and their detailed descriptions.

Table 9: Attack techniques and detailed descriptions used in execution

Attack tactics	Ref.	Attack techniques	Description
Execution	[89]	Application layer protocol	• Installing and running malicious or cracked applications to perform unauthorized activities.
	[90]	Native API	• Execute basic system commands or API calls to enable packet capture on the Ubertooth device, which is responsible for executing functions on the wearable device.
	[91]	Command and scripting interpreter	• Exploit vulnerabilities in applications to execute arbitrary commands.
	[92]	Device synchronization	• During the synchronization process between a wearable device and a paired mobile device, if the data being synchronized contains an executable file, malicious code can be delivered under the guise of a synchronization operation.
	[93]	Firmware update	• The attacker spoofs update notifications or compromises the wearable device's update mechanism to execute a malicious firmware installation of the attacker's choosing.

Persistence is an attack tactic for accessing, working with, or changing the configuration of a wearable device that requires an attacker to have a persistent presence on the device. It includes Boot or Logon Autostart Execution and Subvert Trust Controls attack techniques. Table 10 shows the attack techniques used in the Persistence attack tactic and their detailed descriptions.

Privilege Escalation is an attack tactic that allows an attacker to gain higher levels of privileges on a device and includes Weaken Authentication, Process Injection, and Manipulated Authentication attack techniques. Table 11 shows the attack techniques used in the Privilege Escalation attack tactic and their detailed descriptions.

Table 10: Attack techniques and detailed descriptions used in persistence

Attack tactics	Ref.	Attack techniques	Description
Persistence	[94]	Boot or logon autostart execution	• An attacker configures system settings to automatically run a program during system boot or logon to maintain persistence on a compromised system or gain a higher privilege level. A wearable device is connected to a USB or other device to autorun.
	[95]	Subvert trust controls	• Weaken security controls that warn of untrusted activity or prevent untrusted applications from running.

Table 11: Attack techniques and detailed descriptions used in privilege escalation

Attack tactics	Ref.	Attack techniques	Description
Privilege escalation	[96]	Weaken authentication	• No authentication is performed between wearables and mobile devices, making distinguishing between the attacker's mobile device and the actual user's mobile device is impossible. This allows for persistence or escalation of privileges without re-authentication.
	[97]	Process injection	• Injects a malicious process into a legitimate process to allow the attacker to take control of a Bluetooth-enabled device without the user's knowledge.
	[98]	Manipulated authentication	• To gain user privileges, the attacker manipulates authentication tokens to maintain sessions between wearables and mobile devices.

Defense Evasion is an attack tactic allowing an attacker to evade detection or other defense mechanisms. It includes Weaken Encryption, Disk Content Wipe, Valid Accounts, and Masquerading attack techniques. Table 12 shows the attack techniques used in Defense Evasion attack tactics and their detailed descriptions.

Table 12: Attack techniques and detailed descriptions used in defense evasion

Attack tactics	Ref.	Attack techniques	Description
Defense evasion	[99]	Weaken encryption	• Exploit a vulnerability in the protocol's internal encryption mechanism to compromise the encryption function.
	[100]	Disk content wipe	• It bypasses security features that protect sensitive data by deleting sections responsible for protections needed to lock out external reads and writes to internal flash.
	[101]	Valid accounts	• By bypassing authentication mechanisms, the attacker gains unauthorized access using legitimate credentials without being detected.
	[102]	Masquerading	• Attackers manipulate an object's name, location, or appearance, whether legitimate or malicious, to make it appear legitimate. Examples include phishing firmware update processes and manipulating file metadata.

Credential Access is an attack tactic attackers use to gain unauthorized access to resources. It includes the Unsecured Credentials and Steal Application Access Token attack techniques. Table 13 shows the attack techniques used in the Credential Access attack tactic and their detailed descriptions.

Table 13: Attack techniques and detailed descriptions used in credential access

Attack tactics	Ref.	Attack techniques	Description
Credential access	[103]	Unsecured credentials	• The attacker sniffs wireless communication packets, such as BLE, to access unencrypted credentials or sensitive information transmitted between the wearable device and the paired mobile device.
	[104]	Steal application access token	• The attacker obtains credentials by hijacking the authentication token used to maintain a session between the wearable and mobile device.

Discovery is an attack tactic for gaining information about wearable devices and other network systems. It includes System Information Discovery, Network Service Scanning, Location Tracking,

Passive Sniffing, and Active Sniffing attack techniques. Table 14 shows the attack techniques used in the Discovery tactic and their detailed descriptions.

Table 14: Attack techniques and detailed descriptions used in discovery

Attack tactics	Ref.	Attack techniques	Description
Discovery	[105]	System information discovery	• Obtain information about the system and its components, such as device type and firmware version. Based on this, the attack method is tailored to the vulnerabilities of that version of the wearable device.
	[106]	Network service scanning	• The attacker analyzes packets to retrieve operational details about the device, such as communication protocols or device capabilities.
	[107]	Location tracking	• Through a malicious or exploited application on a compromised wearable device, the attacker can track the device's physical location using standard operating system APIs.
	[108]	Passive sniffing	• The attacker passively intercepts communications without actively participating in the connection. It uses specialized hardware or software tools that can capture packets, but they are difficult to detect.
	[109]	Active sniffing	• Intercepting packages are sent over a network that uses switches.

Lateral Movement is an attack tactic that allows an attacker to gain unauthorized access to and control of remote systems on a network and includes the Use of Alternate Authentication Material, Replication Through Wireless and Remote Services attack techniques. Table 15 shows the attack techniques used in the Lateral Movement attack tactic and their descriptions.

Table 15: Attack techniques and detailed descriptions used in lateral movement

Attack tactics	Ref.	Attack techniques	Description
Lateral movement	[110]	Use alternate authentication material	• An attacker can bypass the standard authentication process to establish control over a wearable device by forcibly pairing it using spoofed authentication credentials.

(Continued)

Table 15 (continued)

Attack tactics	Ref.	Attack techniques	Description
	[111]	Replication through wireless	• Cloning methods via Bluetooth, BLE, WLAN.
	[112]	Remote services	• Exploit vulnerabilities in communication protocols to gain unauthorized access or execute attacks.

Collection is an attack tactic used to identify and collect key information from the target network, such as sensitive files, including user personal information. It includes the Data Local System, Data from Removable Media, Video Capture, Capture Bluetooth Traffic, Adversary-in-the-Middle, and Replay Attack techniques. Table 16 shows the attack techniques and detailed descriptions used in the Collection attack tactic.

Table 16: Attack techniques and detailed descriptions used in collection

Attack tactics	Ref.	Attack techniques	Description
Collection	[113]	Data from local system	• Includes methods that allow the attacker to collect data from the local system. The purpose of this technique is to collect sensitive data that can be used in subsequent phases of the attack. In this technique, the local system is a wearable device.
	[114]	Data from removable media	• It collects sensitive data from all removable media. Data collection can be done automatically by scanning for connected removable media.
	[115]	Video capture	• An attacker can utilize the device's camera to capture video recordings to gather information. Instead of video files, images can be captured at specified intervals.
	[116]	Capture Bluetooth traffic	• Capture Bluetooth traffic from a wearable device using a tool like pcap to collect data without authorization.
	[117]	Adversary-in-the-middle	• Intercept and alter a wearable device's communications. This allows them to manipulate data or collect sensitive data, compromising its integrity and availability.

(Continued)

Table 16 (continued)

Attack tactics	Ref.	Attack techniques	Description
	[118]	Replay attack	• Replay attacks are a common form of attack on wireless communications where an attacker captures legitimate communication packets and later retransmits them with malicious intent. Attacks can include unlocking, sending fake notifications.

Command and Control is an attack tactic for how an attacker communicates with a compromised wearable device or system within a targeted network and includes Communication Through Removable Media, Communication via Bluetooth, and Communication via WLAN attack techniques. Table 17 shows the attack techniques used in the Command and Control attack tactic and their detailed descriptions.

Table 17: Attack techniques and detailed descriptions used in command and control

Attack tactics	Ref.	Attack techniques	Description
Command and control	[119]	Communication through removable media	• An attacker uses removable media to transmit commands from system to system to perform command and control between compromised hosts on a network that may be disconnected.
	[120]	Communication via Bluetooth	• Command and control via Bluetooth communication.
	[121]	Communication via WLAN	• Command and control via WLAN communication.

4.3.3 Attack Result

The Attack Result phase is the final part of the attack process, where the attacker achieves their intended goal. It is related to the state of damage caused by the attack and the impact of the attack and may cause additional damage. Attack Result is categorized into six attack tactics: Exfiltration, Impact, Wearable IoT Service, Wearable IoT Device, Protocol Exploitation, and Effect.

Exfiltration is an attack tactic in which an attacker exfiltrates or causes the removal of sensitive data from a target wearable or mobile device and includes the Transfer Data and Exfiltration Over C2 Channel attack techniques. Table 18 shows the attack techniques used in the Exfiltration attack tactic and their detailed descriptions.

Table 18: Attack techniques and detailed descriptions used in exfiltration

Attack tactics	Ref.	Attack techniques	Description
Exfiltration	[122]	Transfer data	• The collected data is exfiltrated to another device or location controlled by the attacker (the attacker's mobile device).
	[123]	Exfiltration over C2 channel	• When a device connects to a maliciou saccess point, sensitive data intended for a legitimate printer can be redirected and exfiltrated by the attacker. The exfiltrated data is typically sent to an attacker-controlled control and command (C2) setup.

Impact is an attack tactic used by attackers to compromise the availability and integrity of the attack target. It can disrupt or destroy data and systems. It includes the following attack techniques: Delete Device Data, Data Manipulation, Endpoint Denial of Service, Data Encrypted for Impact, Inhibit System Recovery, and Firmware Corruption. Table 19 shows the attack techniques used in the Impact attack tactic and their detailed descriptions.

Table 19: Attack techniques and detailed descriptions used in impact

Attack tactics	Ref.	Attack techniques	Description
Impact	[124]	Delete device data	• Corrupting or disabling sensor data on a wearable device.
	[125]	Data manipulation	• The attacker injects packets to change or add malicious and invalid data, which reduces user confidence in the accuracy and privacy of data on the wearable device.
	[126]	Endpoint denial of service	• The attacker performs an endpoint denial-of-service (DoS) attack on the wearable device to degrade or block service availability to the user.
	[127]	Data encrypted for impact	• The attacker encrypts files stored on the wearable device to prevent users from accessing them.
	[128]	Inhibit system recovery	• The attacker blocks phone service and causes pairing issues, disrupting normal operation and potentially impacting device usability.

(Continued)

Table 19 (continued)

Attack tactics	Ref.	Attack techniques	Description
	[129]	Firmware corruption	• The attacker overwrites or corrupts the contents of flash memory in the system BIOS or other firmware of a system-connected device, rendering the device inoperable or unbootable, thus denying device and/or system usability.

Wearable IoT Service represents the type of service supported by the device. It includes the following attack techniques: Fitness, Medical, Infotainment, Industrial, and Military attack techniques. Table 20 shows the attack techniques used in the Wearable IoT Service attack tactic and their detailed descriptions.

Table 20: Attack techniques and detailed descriptions used in wearable IoT service

Attack tactics	Ref.	Attack techniques	Description
Wearable IoT service	[122]	Fitness	• Target, manipulate or exfiltrate quantified data collected during exercise (e.g., distance, speed, calories burned, heart rate).
	[130]	Medical	• A wearable device that combines wireless body area network (wBAN) and Ubiquitous healthcare technologies. Attacks can prevent them from accurately measuring and communicating the user's physical condition to patients and doctors.
	[131]	Infotainment	• Exploit vulnerabilities in smart glasses, smart watches, to take illegal photos or display false data on the screen interface.
	[132]	Industrial	• Attacks cause problems protecting the body or performing sophisticated tasks in industrial settings.
	[133]	Military	• Wearable devices used for military purposes, such as heart rate monitoring, power delivery, enemy identification, cameras.

Wearable IoT Device represents a type of IoWT device. It includes Accessory, Attachable, and Edible attack techniques. Table 21 shows the attack techniques used in the Wearable IoT Device attack tactic and their detailed descriptions.

Table 21: Attack techniques and detailed descriptions used in wearable IoT device

Attack tactics	Ref.	Attack techniques	Description
Wearable IoT device	[134]	Accessory	• A wearable device in the form of a watch or band, such as a smartwatch, smart band, or smart glasses, is attacked. The attack manipulates the device's data or causes abnormal behavior.
	[135]	Attachable	• A device that is worn on the skin, such as a patch, or in the form of clothing, such as smart shoes or clothing, is a smart device. When an attack is executed, the device's data is manipulated to show false output values.
	[136]	Eatable	• Devices that are implanted or taken directly into the body, such as smart pills, can be attacked, resulting in actual human harm.

Protocol Exploitation is an attack tactic for exploiting vulnerable protocols in wearable device communications. It includes BLE, Wi-Fi Direct, NFC, Zigbee, LTE-M, NB-IoT, and NR-REDCAP attack techniques. Table 22 shows the attack techniques used in the Protocol Exploitation attack tactic and their detailed descriptions.

Table 22: Attack techniques and detailed descriptions used in protocol exploitation

Attack tactics	Ref.	Attack techniques	Description
Protocol exploitation	[137]	BLE	• Attacks that exploit vulnerabilities in BLE.
	[138]	Wi-Fi direct	• Attacks that exploit vulnerabilities in Wi-Fi direct.
	[139]	NFC	• Attacks that exploit vulnerabilities in NFC.
	[140]	Zigbee	• Attacks that exploit vulnerabilities in Zigbee.
	[141]	LTE-M	• Attacks that exploit vulnerabilities in LTE.
	[142]	NB-IoT	• Attacks that exploit vulnerabilities in NB-IoT.

(Continued)

Table 22 (continued)

Attack tactics	Ref.	Attack techniques	Description
	[143]	NR-REDCAP	• Attacks that exploit vulnerabilities in NR-REDCAP.

Effect is an attack tactic related to damage caused by a wearable device attack and includes the IoWT Device Damage and Physical Injury attack techniques. Table 23 shows the attack techniques used in the Effect attack tactic and their detailed descriptions.

Table 23: Attack techniques and detailed descriptions used in effect

Attack tactics	Ref.	Attack techniques	Description
Effect	[144]	IoWT device damage	• IoWT device data is corrupted or disabled, preventing the device from being used normally (e.g., displaying inaccurate measurements due to health data manipulation).
	[114]	Physical injury	• Actual physical harm is caused to a person due to an attack on an IoWT device (e.g., medical errors due to abnormal behavior of a medical device)

4.4 Step 3: Developed IWTW Framework

Fig. 3 shows the IWTW framework developed by combining the 3 Attack Categories, 18 Attack Tactics, and 68 Attack Techniques for the attack flows derived from Sections 4.2 and 4.3. The attack categories are organized as follows: Launch on Attack, Expand Attack, Attack Result. Launch on Attack indicates a security threat that may occur in the early stages of an attack. Therefore, the subsections are organized as follows: Reconnaissance, Resource Development, and Initial Access. Expand Attack refers to expanding the attack process to the attacker's intended target. Accordingly, the subsections are organized as follows: Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control. Attack Result indicates the damage caused by the attack and its impact. Therefore, the subsections are organized as follows: Exfiltration, Impact, Wearable IoT Service, Wearable IoT Device, Protocol Exploitation, and Effect. IoWT attack techniques included in each subsection were derived and mapped to attack tactics through the following process: 1. Analyze attack cases targeting IoWT assets. 2. Categorize IoWT by asset type, attack process, and security threat. 3. Classify potential security threats that may occur targeting IoWT. 4. Analyze and standardize the main functions that constitute security threats.

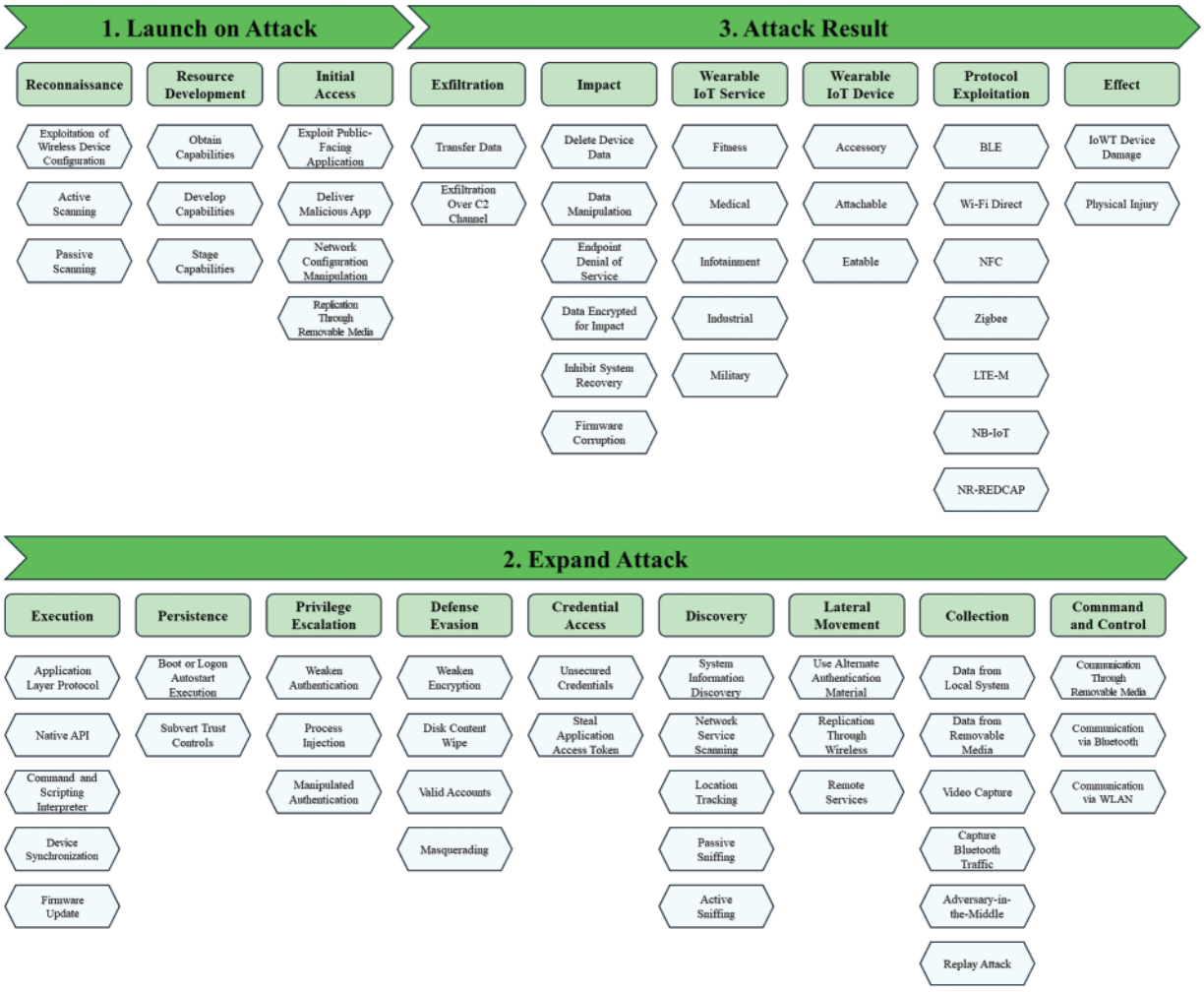

Figure 3: Overview of IWTW framework

Figs. 4–6 show the IWTW framework's attack categories: Launch on Attack, Expand Attack, Attack Result, and Components.

Launch on Attack is a category of security threats and attacks that can occur at the beginning of an attack in the IWTW framework. Its attack tactics are Reconnaissance, Resource Development, and Initial Access. The Launch on Attack category has 10 attack techniques, including the information and tools used to carry out the attack, and represents the attack vector for initial access.

Expand Attack is a category of attacks that extends the attack process to the attacker's intended target after initial access in the IWTW framework. It consists of the following attack tactics: Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, and Command and Control. There is a total of 33 attack tactics that fall under the Expand Attack category. They perform tasks to achieve the attack goal, such as remotely executing malicious actions against IoWT devices or gaining high privileges and persisting in the system based on them, avoiding attack detection, or communicating with and controlling systems inside the network, collecting key data within the IoWT device, or obtaining information.

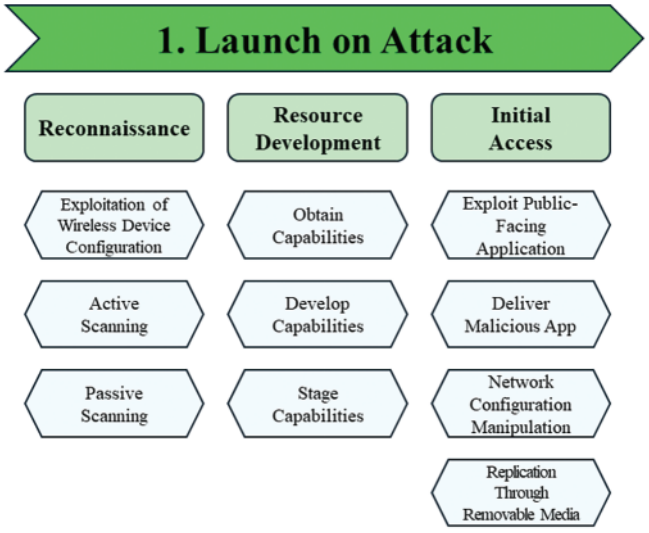

Figure 4: Attack category of IWTW framework, launch on attack

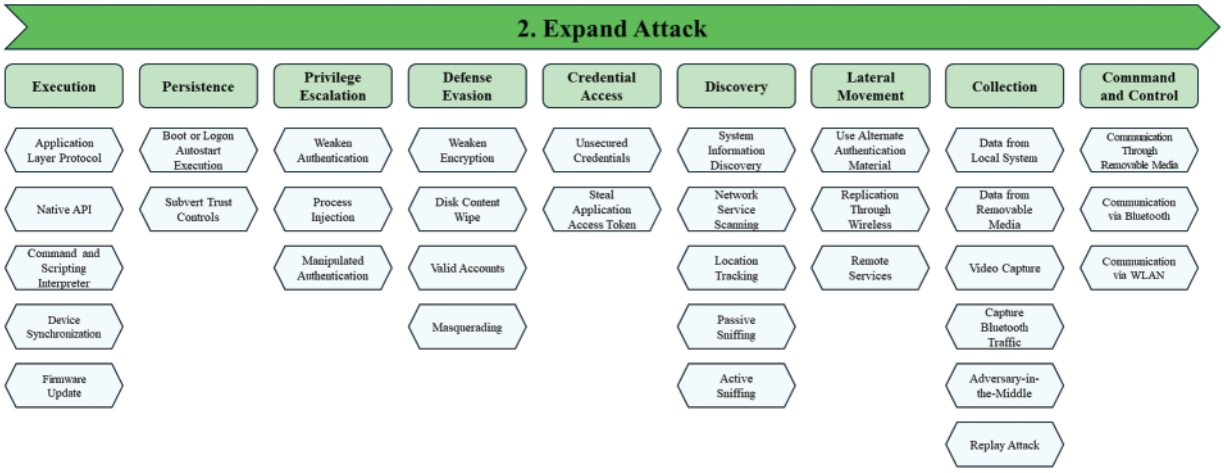

Figure 5: Attack category of IWTW framework, expand attack

Attack Result is a category of attack that achieves the attacker's intended goal in the IWTW framework. It is composed of the following attack tactics: Exfiltration, Impact, Wearable IoT Service, Wearable IoT Device, Protocol Exploitation, and Effect. There is a total of 25 attack tactics in the Attack Result attack category, which compromise the availability and integrity of services and data in IoWT devices.

The IWTW framework is highly reliable because it only includes attack techniques that can be performed against IoWT devices. The addition of new attack tactics allows for more detailed cybersecurity threat analysis.

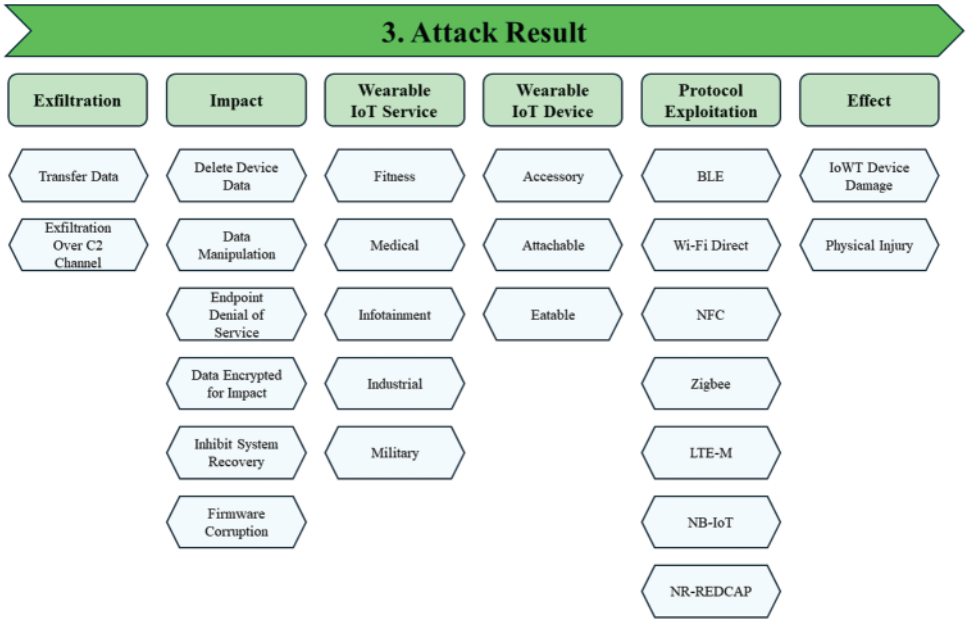

Figure 6: Attack category of IWTW framework, attack result

5 Case Study

Section 5 verifies the proposed method by applying the proposed IWTW framework to three actual attack cases targeting various IoWT devices. Through a case study, we confirm whether the IWTW framework can classify IoWT assets, attack processes, security threats, and attack tactics and techniques.

5.1 Case Study 1: MiBand 2

Fig. 7 illustrates how the MiBand 2 smart band attack case is applied to the IWTW framework. Exploitation of Wireless Device Configuration: Filtered and analyzed BLE communication wireless network traffic to analyze source and destination addresses. Active Scanning: Discovered wearable devices through the discovery capabilities of BLE sniffers. Obtain Capabilities: Uses the application and hardware sniffers required for the attack. Masquerading: Display a user authentication screen with fake commands. Passive Sniffing: Sniffs the MiBand 2's packets through the SmartRF Sniffer. Data from Local System: Using BLETestTool to collect sports and heart rate data from MiBand 2. Capture Bluetooth Traffic: Capture BLE communication packets. Adversary-in-the-Middle: Intercept sensitive data between wearable device communications. Replay Attack: vibrates the MiBand 2 with a fake notification. Communication via Bluetooth: Communicates with the attacker based on Bluetooth. Transfer Data: Leaks collected data to the attacker's device. Inhibit System Recovery: Prevents phone and text services from functioning normally through fake notifications. Fitness: Fitness data related to exercise is leaked. Infotainment: Vulnerabilities in smart bands are exploited. Accessory: A wearable device in a wearable form. BLE: An attack that exploits a vulnerability in BLE communication. IoWT Device Damage: The MiBand was physically damaged by the constant vibration caused by the fake notifications.

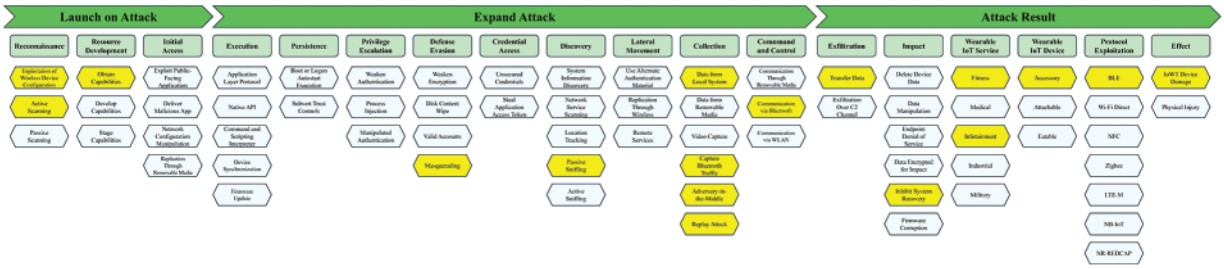

Figure 7: IWTW framework applied to MiBand 2 smart band attack

Zhang et al. [145] used the CC2540 USB, TI SmartRF, and BLETestTool to remotely sniff and analyze traffic on the MiBand 2 wearable smartband. Fig. 8 shows an overview of the attack process for MiBand 2. The CC2540 USB dongle is used as a hardware sniffer, TI SmartRF Packet Sniffer is a software application that sniffs BLE communication packets between the smartphone and the wearable device, and BLETestTool is an attack tool that runs on an Android smartphone to test attacks against the wearable device. First, the hardware sniffer, smartphone, and smart wristband are placed close to Bluetooth discovery so the smartphone can discover the MiBand 2 via Bluetooth. Then, turn on the TI SmartRF Packet Sniffer on your PC and launch the MiBand 2's official support application on your Android phone. The packets are sniffed once connected to the MiBand 2 through the application, and the information is displayed on the TI SmartRF Packet Sniffer. All sniffed packets are stored in hexadecimal, and the commands in the packets are analyzed by converting them to decimal, ASCII code, Unicode, or UTF-8 code. After running BLETestTool on an Android smartphone and using it to connect to the MiBand 2, send some commands recorded using BLETestTool to the MiBand 2 and fake commands written by the attacker to bypass the authentication process. Once the authentication process is complete, the attacker uses BLETestTool to perform attacks such as getting sports and heart rate data or vibrating this MiBand 2 with fake notifications.

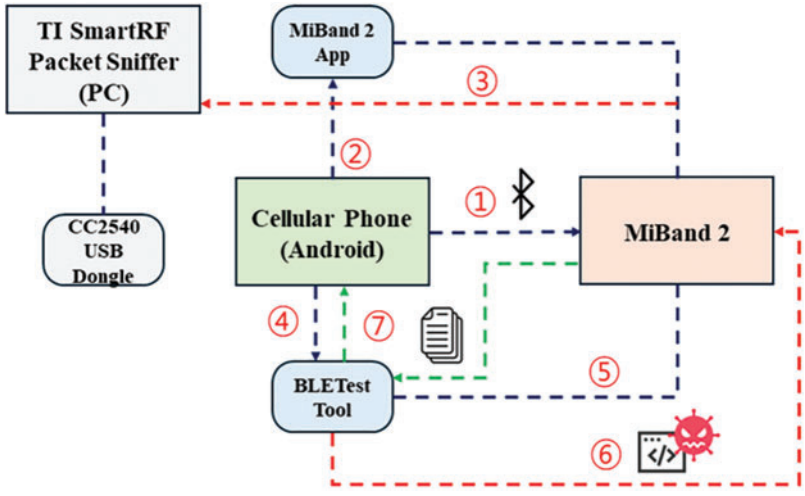

Figure 8: Overview of the MiBand 2 attack process

5.2 Case Study 2: Fitbit Charge HR|Surge, Samsung Gear 3, Xiaomi Amazifit

Fig. 9 illustrates how the Smartwatch/band based on BLE 4.0 and 4.2 attack case is applied to the IWTW framework. Exploitation of Wireless Device Configuration: Filtered and analyzed BLE communication wireless network traffic to analyze source and destination addresses. Active Scanning: Scanned for wearable devices through a BLE sniffer. Obtain Capabilities: the HCI snoop log is the tool used in the attack. The Native API enables packet capture from Ubertooth devices. Weaken Encryption: Weaknesses in the data encryption mechanism result in plaintext transmission. Unsecured Credentials: Uses the user's digital signature. System Information Discovery: Identifies devices through packet analysis. Passive Sniffing: Sniffs packets from the wearable device through an Adafruit sniffer. Use Alternate Authentication Material: Use a spoofed digital signature to maintain connectivity between devices. Data from Local System: Perform follow-up attacks based on sender and receiver MAC addresses and identifying devices derived through WireShark. Capture Bluetooth Traffic: Captures BLE communication packets. Adversary-in-the-Middle: Intercept sensitive information such as sender and receiver static MAC addresses and communication messages between wearable device communications. Communication via Bluetooth: Communicates with the attacker based on Bluetooth. Transfer Data collects data information about the wearer's movements and habits. Fitness: Fitness data related to the wearer's movements is compromised. Infotainment: A vulnerability in the smartwatch or band has been exploited. Accessory: A wearable device in a wearable form. BLE: The attack exploits a vulnerability in BLE communication.

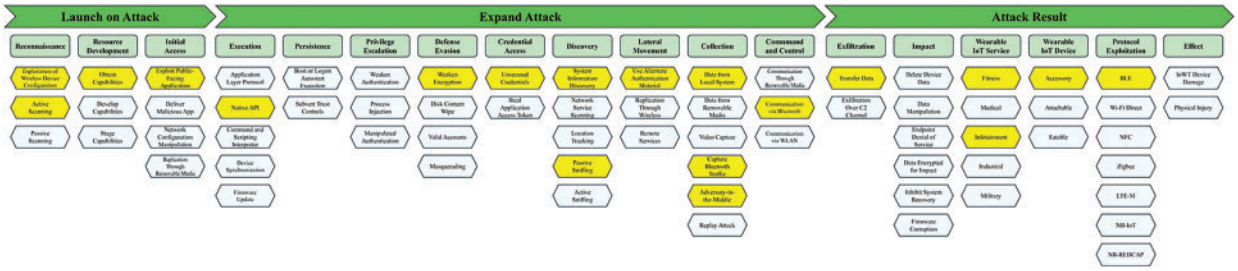

Figure 9: IWTW framework applied to smartwatch/band based on BLE 4.0 and 4.2 attack

Cusack et al. [146] used BLE sniffers to capture and analyze communication packets from Fitbit Charge HR/Surge, Samsung Gear 3, Xiaomi Amazifit smartwatches, and smartbands using BLE 4.0 and 4.2 to extract sensitive information. Fig. 10 shows an overview of the attack process for Fitbit Charge HR/Surge, Samsung Gear 3, and Xiaomi Amazifit attack process. First, use Ubertooth, the HCI snoop log, and the Adafruit sniffer tool to dump the pairing-related packets of the wearable devices into pcapng and pcap files. The dumped files are analyzed using Wireshark to check whether the data is text-encrypted and to collect essential information such as digital signatures, device identification, mapping of the wearer's movements and habits, and device logs. As a result, sensitive information, such as static MAC addresses of the sender and receiver, and communications messages, were sent in plain text, and message logs (Email, SMS, and Facebook) were checked. The vulnerability allows for blueprinting attacks against each wearable device. Analysis showed that all wearable devices had credential data that provided access.

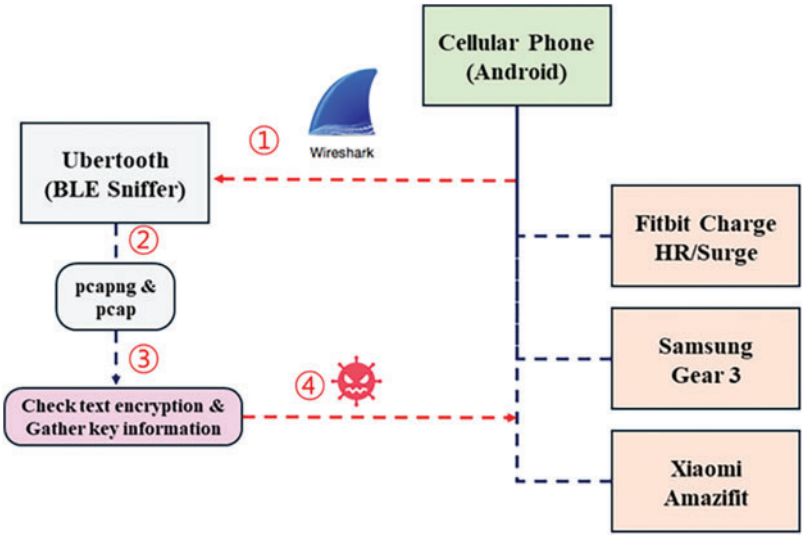

Figure 10: Overview of the Fitbit Charge HR/Surge, Samsung Gear 3, Xiaomi Amazifit attack process

5.3 Case Study 3: Honor Band 5 Honor Watch ES

Fig. 11 illustrates how the Honor Band 5 and Honor watch ES smart watch attack case is applied to the IWTW framework. Exploitation of Wireless Device Configuration: Filtered and analyzed BLE communication wireless network traffic. Active Scanning: Discovered wearable devices through the BLE sniffer's discovery capabilities. Obtain Capabilities: The Nordic Semiconductor nRF52 DK Sniffer tool was used in the attack. Weaken Authentication: No encryption during the pairing process. System Information Discovery: Identifies devices by deriving plain text data through packet analysis. Passive Sniffing: Sniffing packets through a BLE sniffer. Data from Local System: The attacker used Wireshark to collect plain text data about personal information from a series of Honor devices. Capture Bluetooth Traffic: Capture BLE communication packets. Adversary-in-the-Middle: Intercept sensitive information such as physical activity data, synchronization, connection, and reconnection data between wearable device communications. Communication via Bluetooth: Communicates with an attacker based on Bluetooth. Transfer Data: Collect sensitive personal information. Infotainment: Vulnerabilities in the smartwatch/band are exploited. Accessory: A wearable device that can be worn. BLE: An attack that exploits a vulnerability in BLE communication.

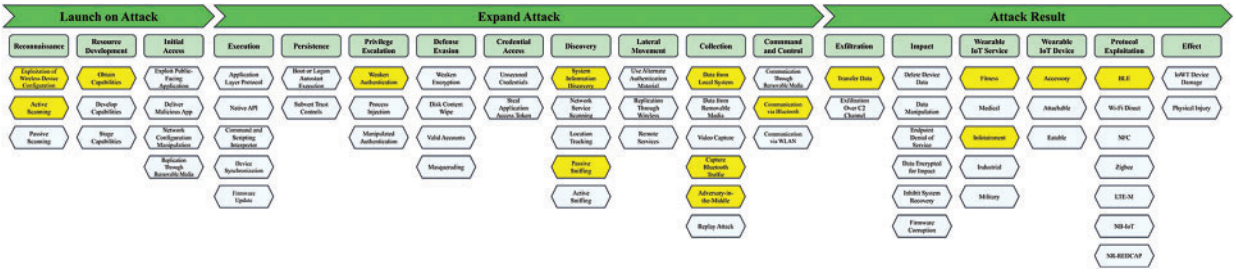

Figure 11: IWTW framework applied to Honor Band 5 and Honor watch ES smart watch attack

Fuster et al. [70] used the Nordic Semiconductor nRF52 DK Sniffer to capture and analyze communication packets from various wearable smartwatches/bands to derive privacy and security vulnerabilities. In Case Study 3, They focus on the Honor Band 5 and Honor Watch ES devices. Fig. 12 shows an overview of the attack process for Honor Band 5 and Honor Watch ES attack process. First, capture BLE communication between wearable and mobile devices using the Nordic Semiconductor nRF52 DK tool and then analyze it using WireShark. BLE communication is performed via pairing, and physical activity data, synchronization, connection, and reconnection data are collected and analyzed. Honor device series require a separate Huawei ID and Huawei Health service to use. The devices use unencrypted pairing methods and communication, which expose personal data in plain text. In addition, wearable devices can be identified by using static MAC addresses.

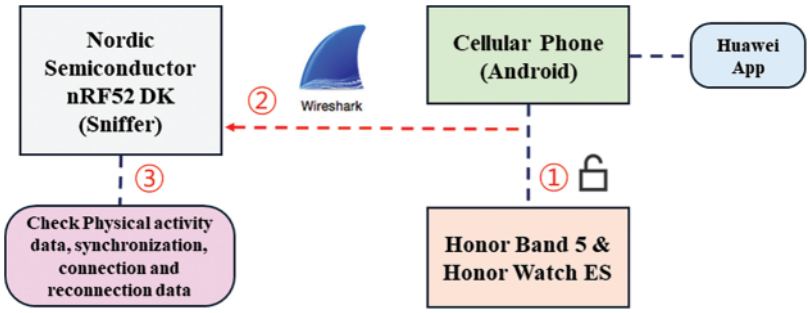

Figure 12: Overview of the Honor Band 5 and Honor Watch ES attack process

5.4 Case Study 4: Senbono CF-58

Fig. 13 illustrates how the Senbono CF-58 smart watch attack case is applied to the IWTW framework. Exploitation of Wireless Device Configuration: Filtered and analyzed BLE communication wireless network traffic. Active Scanning: Discovered wearable devices through the BLE sniffer's discovery capabilities. Obtain Capabilities: The BetterCap Sniffer tool was used in the attack. Command and Scripting Interpreter: Gather details using the BLE.enum command. Weaken Encryption: No encryption during network connection. System Information Discovery: Identifies devices by deriving plain text data through packet analysis. Passive Sniffing: Sniffing packets through the BetterCap sniffer. Data from Local System: The attacker used Wireshark to collect plain text data about personal information from the Senbono CF-58 devices. Capture Bluetooth Traffic: Capture BLE communication packets. Adversary-in-the-Middle: Intercept sensitive information such as physical activity data, synchronization, connection, and reconnection data between wearable device communications. Communication via Bluetooth: Communicates with an attacker based on Bluetooth. Data Manipulation: Change data by modifying the descriptor of the UUID. Infotainment: Vulnerabilities in the smartwatch/band are exploited. Accessory: A wearable device that can be worn. BLE: An attack that exploits a vulnerability in BLE communication.

Khan et al. [147] used BetterCap Sniffer to capture smartwatch communication packets and GattTool to establish and control connections between BLE gadgets. In Case Study 4, They focus on Senbono CF-58 devices. Fig. 14 shows an overview of the attack process for the Senbono CF-58 devices attack process. First, install the BetterCap BLE scanning tool on your Kali Linux machine and enable the Bluetooth service. After identifying the BLE device through BetterCap, find the Senbono CF-58 device in the list of scanned BLE devices and record its MAC address. Afterward, the Mac address is collected, and the BLE.enum command collects detailed information. After completing

attack reconnaissance, check the data packets through Wireshark. Send a ping to the BLE gadget to capture packets and analyze the gadget's UUID descriptor model. Check what type of data the gadget's UUID descriptor corresponds to. Connect your CF58 smartwatch and Kali Linux machine using GATTTOOL. Also, access the terminal and check all UUIDs associated with the device. Afterward, used Wireshark to cross-reference the previously identified UUIDs to identify specific UUIDs to target. Finally, the data on the smartwatch is altered by modifying the value of the target UUID.

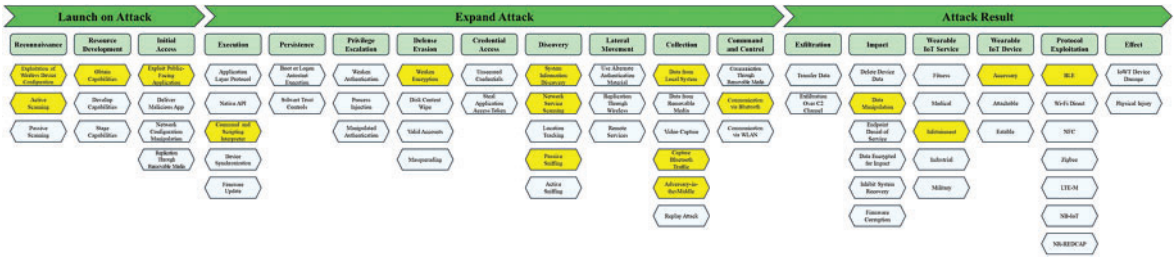

Figure 13: IWTW framework applied to Senbono CF-58 smart watch attack

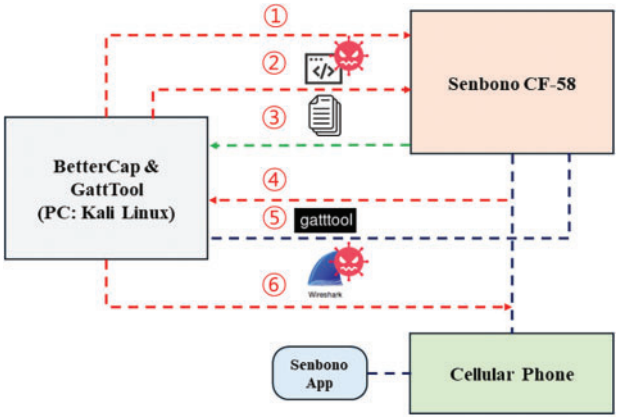

Figure 14: Overview of the Senbono CF-58 attack process

6 Discussion

In this session, we compare and analyze IWTW and existing cyber threat framework research. We selected evaluation items that could compare threat modeling and framework characteristics for comparative analysis: compare domain, Threat granularity, Threat, Standardization, and Applicability in the IoWT. Table 24 compares the proposed framework with existing research.

Table 24: Comparison of cyber threat framework, including ours

Reference	Domain	Threat granularity	Threat	Standardization	Applicability in the IoWT
BLE threat model [8]	IoWT	High	17	O	O
ERMO [9]	IT, IoT	Low	2	X	X

(Continued)

Table 24 (continued)

Reference	Domain	Threat granularity	Threat	Standardization	Applicability in the IoWT
MITRE ATT&CK [10]	IT, mobile	High	86 (mobile)	O	△
CONCORDIA–CMTMF [11]	Mobile	High	47	O	△
WSHD threat model [12]	IoWT	Low	7	X	O
MEDICALHARM [13]	IoWT	Low	11	O	O
Emerging MWBD [30]	IT, IoT	Low	8	X	X
Bhadra [31]	Mobile	High	55	O	△
Ours (IWTW)	IoWT	High	68	O	O

This research proposed IWTW framework to analyze cyber threats targeting IoWT devices. The proposed IWTW was studied in cyber threat frameworks (BLE Threat Model [8], ERMO [9], MITER ATT&CK [10], CONCORDIA–CMTMF [11], WSHD Threat Model [12], MEDICALHARM [13], Emerging MWBD [30], Bhadra [31]), as shown in Table 24.

ERMO, Emerging MWBD, MITER ATT&CK, and CONCORDIA–CMTMF analyze security threats targeting IT, IoT, and mobile. Although some attack tactics and techniques were suitable for use in an IoWT environment, not all components could be applied. ERMO, Emerging MWBD, WSHD Threat Model, and WSHD Threat Model did not perform a too comprehensive threat modeling process or provide detailed information on detailed attack tactics and techniques for security threats. Most frameworks with low threat granularity had a small number of threats. In the case of the BLE Threat Model, the threat granularity is high, but the number of threats is small because a limited threat model targeting only a single protocol was proposed. ERMO, Emerging MWBD, and WSHD Threat Model do not consider the formalization process for security threat analysis, so it is unclear whether accurate threat identification is possible.

The IWTW framework presented in this research is designed to analyze cybersecurity threats targeting IoWT devices. For detailed analysis of security threats, IoWT assets, attack processes, and security threats from actual IoWT attack cases were derived. Additionally, a standardization was conducted to classify attack tactics and techniques. In addition, through a case study on actual IoWT attack cases, we verified that the IWTW framework can effectively classify IoWT security threats.

The IWTW framework allows detailed analysis of cyber threats to IoWT. However, the IWTW framework has several limitations. In this research, we investigated actual IoWT attack cases and potential security threats that could occur in IoWT to derive security threats. As attack methods become more sophisticated and new attack techniques are used, the existing IWTW framework alone may have a negative impact on analyzing cyber-attacks. Additionally, there are limits to the attack

tactics and techniques that can be analyzed depending on the attack cases investigated and the scale of the security threat. Therefore, continuous updating of the IWTW framework is necessary.

7 Conclusion

As IoWT technology has evolved, the sensors embedded in wearable devices have become smaller and more accessible through low-power mobile networks. However, these features also give IoWT devices limited processing power and bandwidth, which prevents the use of high computational security mechanisms such as AES and RSA. Existing works propose threat modeling or frameworks targeting IoT or low-power protocols. However, the proposed techniques only apply to specific protocols, the models are too comprehensive, and they do not consider the IoWT environment. Therefore, the threat model presented in the existing research on cyber threat analysis and modeling for IoWT is specialized for specific devices. In addition, it is difficult to identify attacks quickly because it does not present standardized attack tactics and techniques. For these reasons, this research proposes IWTW, a framework for cyber threat analysis for IoWTs. The methodology for developing the IWTW framework is divided into two areas: Clustering and Development. Clustering stores data derived from analyzing attack cases against IoWTs and potential security threats that may occur in IoWTs. It consists of two parts: Analysis and Standardization. The Analysis part includes IoWT Attack Cases, which analyzes attack cases that can occur against IoWT, and IoWT Security Threat, which analyzes potential security threats that can occur in IoWT. IoWT Attack Cases is based on actual attacks against IoWT and analyzes the attack process and security threats. IoWT Security Threat analyzes the security threats that can be caused by potential attackers targeting IoWT. The Standardization part performs the process of standardizing the attack categories, attack tactics, and attack techniques derived from the Analysis part. The development combines the formalized attack categories, attack tactics, and attack techniques from the Clustering section to derive an IWTW framework. ITWT framework was validated through four case studies targeting MiBand 2, Fitbit Charge HR/Surge, Samsung Gear 3, Xiaomi Amazifit, Honor Band 5, Honor Watch ES, and Senbono CF-58 devices. For the comparative analysis of IWTW and existing cyber threat framework studies, we selected evaluation items that allow us to compare threat modeling and framework characteristics: comparison domain, threat granularity, threat, standardization, and IoWT applicability. We confirmed that the IWTW framework can classify IoWT security threats more effectively than existing studies. We discussed the attack cases investigated for security threats and the limitations of the attack techniques that can be analyzed when the scale is small. As attack methods become more sophisticated and new techniques are used, the existing IWTW framework alone may negatively impact the analysis process. Therefore, continuous updating of the IWTW framework is necessary.

In future research, we will regularly update the IWTW framework to increase the scale of attack tactics and techniques that can be analyzed. Meanwhile, we will develop a new framework for advancing IoWT attack technology and responding to IoWT security threats by building an IoWT testbed and conducting vulnerability analysis research through attack simulation.

Acknowledgement: None.

Funding Statement: This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No. RS-2021-II210493, 5G Massive Next Generation Cyber Attack Deception Technology Development, 90%), and the Gachon University research fund of 2022 (GCU-202300750001, 10%).

Author Contributions: Conceptualization, GyuHyun Jeon; methodology, GyuHyun Jeon and Hojun Jin; Case study, GyuHyun Jeon and Ju Hyeon Lee; writing, GyuHyun Jeon; writing-review and editing, Ju Hyeon Lee, Seungho Jeon, and Jung Taek Seo. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Dian FJ, Vahidnia R, Rahmati A. Wearables and the Internet of Things (IoT), applications, opportunities, and challenges: a survey. IEEE Access. 2020;8:69200–11. doi:10.1109/ACCESS.2020.2986329.
2. Cornacchia M, Ozcan K, Zheng Y, Velipasalar S. A survey on activity detection and classification using wearable sensors. IEEE Sens J. 2016;17(2):386–403. doi:10.1109/JSEN.2016.2628346.
3. Tahir H, Tahir R, McDonald-Maier K. On the security of consumer wearable devices in the Internet of Things. PLoS One. 2018;13(4):e0195487. doi:10.1371/journal.pone.0195487.
4. Hale ML, Lotfy K, Gamble RF, Walter C, Lin J. Developing a platform to evaluate and assess the security of wearable devices. Digit Commun Netw. 2019;5(3):147–59. doi:10.1016/j.dcan.2018.10.009.
5. Cirani S, Picone M. Wearable computing for the internet of things. IT Prof. 2015;17(5):35–41. doi:10.1109/MITP.2015.89.
6. Gupta A, Tripathi M, Sharma A. A provably secure and efficient anonymous mutual authentication and key agreement protocol for wearable devices in WBAN. Comput Commun. 2020;160:311–25. doi:10.1016/j.comcom.2020.06.010.
7. Zhang C, Shahriar H, Riad AK. Security and privacy analysis of wearable health device. In: 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), 2020; Madrid, Spain: IEEE.
8. Barua A, Al Alamin MA, Hossain MS, Hossain E. Security and privacy threats for bluetooth low energy in IoT and wearable devices: a comprehensive survey. IEEE Open J Commun Soc. 2022;3:251–81.
9. Griffy-Brown C, Miller H, Chun M, Johnson K. Cyber risk case analysis in wearables and medical devices: developing a cyberbio security risk framework. In: Portland International Conference on Management of Engineering and Technology (PICMET), 2022; Portland, OR, USA: IEEE.
10. Mobile matrix: MITRE ATT&CK; 2024. Available from: https://attack.mitre.org/matrices/mobile/. [Accessed 2024].
11. Santos B, Barriga L, Dzogovic B, Hassan I, Feng B, Jacot N, et al., editors. Threat modelling for 5G networks. In: 2022 International Wireless Communications and Mobile Computing (IWCMC), 2022; Dubrovnik, Croatia: IEEE.
12. Timko D, Sharko M, Li Y. Security analysis of wearable smart health devices and their companion apps. In: 2024 IEEE Security and Privacy Workshops (SPW), 2024.
13. Kwarteng E, Cebe M. MEDICALHARM: a threat modeling designed for modern medical devices and a comprehensive study on effectiveness, user satisfaction, and security perspectives. Int J Inf Secur. 2024;23(3):2225–68.
14. Qureshi N, Shin D. Performance analysis of IoT-enabled DDoS botnets in wearable devices. J Theor Appl Inf Technol. 2021;99(16):4026–43.

15. Aroganam G, Manivannan N, Harrison D. Review on wearable technology sensors used in consumer sport applications. Sensors. 2019;19(9):1983. doi:10.3390/s19091983.
16. Seneviratne S, Hu Y, Nguyen T, Lan G, Khalifa S, Thilakarathna K, et al. A survey of wearable devices and challenges. IEEE Commun Surv Tutor. 2017;19(4):2573–620.
17. Wi-Fi Direct: WiFi ALLIANCE. Available from: https://www.wi-fi.org/discover-wi-fi/wi-fi-direct [Accessed 2024].
18. What is the difference between bluetooth and 2.4 GHz? MeeTion; 2023. Available from: https://www.meetion.com/what-is-the-difference-between-bluetooth-and-24-ghz.html. [Accessed 2024].
19. ISO/IEC 14443-4:2018; 2018. Available from: https://www.iso.org/standard/73599.html. [Accessed on 2024].
20. Compatibility PB. IEEE standard for low-rate wireless networks. 2023. Available from: https://ieeexplore.ieee.org/abstract/document/10014667. [Accessed 2024].
21. Release 15: 3GPP; 2019. Available from: https://www.3gpp.org/specifications-technologies/releases/release-15. [Accessed 2024].
22. Release 17: 3GPP; 2022. Available from: https://www.3gpp.org/specifications-technologies/releases/release-17 [Accessed 2024].
23. Panicacci S, Giuffrida G, Donati M, Lubrano A, Ruiu A, Fanucci L. editors. Empowering home health monitoring of COVID-19 patients with smartwatch position and fitness tracking. In: 2021 IEEE 34th International Symposium on Computer-Based Medical Systems (CBMS), 2021; Aveiro, Portugal: IEEE.
24. Collotta M, Pau G, Talty T, Tonguz OK. Bluetooth 5: a concrete step forward toward the IoT. IEEE Commun Mag. 2018;56(7):125–31.
25. Bhatti DS, Saleem S, Imran A, Iqbal Z, Alzahrani A, Kim H, et al. A survey on wireless wearable body area networks: a perspective of technology and economy. Sensors. 2022;22(20):7722. doi:10.3390/s22207722.
26. Darwish A, Hassanien AE. Wearable and implantable wireless sensor network solutions for healthcare monitoring. Sensors. 2011;11(6):5561–95. doi:10.3390/s110605561.
27. Sun H, Zhang Z, Hu RQ, Qian Y. Wearable communications in 5G: challenges and enabling technologies. IEEE Vehicular Technol Mag. 2018;13(3):100–9.
28. Bello Y, Figetakis E. Iot-based wearables: a comprehensive survey. arXiv preprint arXiv:2304.09861. 2023.
29. Lee J, Kim D, Ryoo H-Y, Shin B. Sustainable wearables: wearable technology for enhancing the quality of human life. Sustainability. 2016;8(5):466. doi:10.3390/su8050466.
30. Jian S. Industrial design of wearable intelligent devices based on wireless networks. Meas: Sens. 2023;30:100934. doi:10.1016/j.measen.2023.100934.
31. Academy CN. Introduction to networks companion guide. 1 edition. San Jose, CA, USA: CISCO; 2013.
32. Vakhter V, Soysal B, Schaumont P, Guler U. Threat modeling and risk analysis for miniaturized wireless biomedical devices. IEEE Internet Things J. 2022;9(15):13338–52. doi:10.1109/JIOT.2022.3144130.
33. Rao SP, Chen H-Y, Aura T. Threat modeling framework for mobile communication systems. Comput Secur. 2023;125(5):103047. doi:10.1016/j.cose.2022.103047.
34. Silva-Trujillo AG, González González MJ, Rocha Pérez LP, García Villalba LJ. Cybersecurity analysis of wearable devices: smartwatches passive attack. Sensors. 2023;23(12):5438. doi:10.3390/s23125438.
35. Lee M, Lee K, Shim J, S-j Cho, Choi J. Security threat on wearable services: Empirical study using a commercial smartband. In: 2016 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), 2016; Seoul, Republic of Korea: IEEE.
36. Langone M, Setola R, Lopez J. Cybersecurity of wearable devices: an experimental analysis and a vulnerability assessment method. In: 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), 2017; Turin, Italy: IEEE.
37. Siboni S, Shabtai A, Elovici Y. Leaking data from enterprise networks using a compromised smartwatch device. In: Proceedings of the 33rd Annual ACM Symposium on Applied Computing, 2018; Pau, France.

38. Goyal R, Dragoni N, Spognardi A. Mind the tracker you wear: a security analysis of wearable health trackers. In: Proceedings of the 31st Annual ACM Symposium on Applied Computing, 2016; Pisa, Italy.
39. Arias O, Wurm J, Hoang K, Jin Y. Privacy and security in internet of things and wearable devices. IEEE Trans Multi-Scale Comput Syst. 2015;1(2):99–109. doi:10.1109/TMSCS.2015.2498605.
40. Lotfy K, Hale ML. Assessing pairing and data exchange mechanism security in the wearable internet of things. In: 2016 IEEE International Conference on Mobile Services (MS), 2016; San Francisco, CA, USA: IEEE.
41. Yan Y, Qian Y, Sharif H, Tipper D. A survey on cyber security for smart grid communications. IEEE Commun Surv Tutor. 2012;14(4):998–1010. doi:10.1109/SURV.2012.010912.00035.
42. Mejri MN, Ben-Othman J, Hamdi M. Survey on VANET security challenges and possible cryptographic solutions. Vehicular Commun. 2014;1(2):53–66. doi:10.1016/j.vehcom.2014.05.001.
43. Zuo C, Wen H, Lin Z, Zhang Y. Automatic fingerprinting of vulnerable ble iot devices with static uuids from mobile apps. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 2019; London, UK.
44. Security Advisory. Identity authentication bypass vulnerability in the Huawei children smart watch (Simba-AL00); HUAWEI; 2023. Available from: https://www.huawei.com/en/psirt/security-advisories/2023/huawei-sa-iabvithcswsa-c385b2dc-en [Accessed 2024].
45. Riad AKI, Shahriar H, Zhang C, Barsha FL. Heath device security and privacy: a comparative analysis of Fitbit, Jawbone, google glass and samsung galaxy watch. In: Data protection and privacy in healthcare. 2021; Boca Raton, FL, USA: CRC Press; p. 91–108.
46. Ai M, Xue K, Luo B, Chen L, Yu N, Sun Q, et al. Blacktooth: breaking through the defense of bluetooth in silence. In: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, 2022; Los Angeles, CA, USA.
47. Singh N, Buyya R, Kim H. Securing cloud-based internet of things: challenges and mitigations. arXiv preprint arXiv:2402.00356. 2024.
48. Contini MS, Martins LEG. Wearable device sensing technologies: a systematic literature review: analysis of sensors applicable to wearable devices. Res Biomed Eng. 2024;40(1):69–84.
49. Paul A, Sinha S. Denial of service attacks in the internet of things. In: Internet of Things in modern computing. 2023; Boca Raton, FL, USA: CRC Press; p. 67–90.
50. Bakhshi T, Ghita B, Kuzminykh I. A review of IoT firmware vulnerabilities and auditing techniques. Sensors. 2024;24(2):708. doi:10.3390/s24020708.
51. Praveen P, Singh RK. Smart devices and SRAM: analyzing their impact. In: 2023 International Conference on Sustainable Emerging Innovations in Engineering and Technology (ICSEIET), 2023; Ghaziabad, India: IEEE.
52. Bang S, Jang J, Ro M, Choi Y, Kwon D, Lee K, et al. Evaluating LoRaWAN performance in intentional and unintentional DoS attacks by legacy 900MHz network devices. In: 2023 6th International Conference on Advanced Communication Technologies and Networking (CommNet), 2023; Rabat, Morocco: IEEE.
53. Sen ERK, Dash EA. Unveiling the shadows: exploring the security challenges of the internet of things (IoT). Int J Scientific Res Manag. 2023;7(7):1–12. doi:10.55041/IJSREM23970.
54. Lee J, Lee K. Spy in your eye: spycam attack via open-sided mobile VR device. IEICE Trans Inf Syst. 2022;105(10):1817–20.
55. Zhang N, Yuan K, Naveed M, Zhou X, Wang X. Leave me alone: App-level protection against runtime information gathering on android. In: 2015 IEEE Symposium on Security and Privacy, 2015; San Jose, CA, USA: IEEE.
56. Cyr B, Horn W, Miao D, Specter M. Security analysis of wearable fitness devices (Fitbit), Cambridge, Massachusetts, USA: Massachusetts Institute of Technology; 2014. vol. 1, p. 1–14.

57. Givehchian H, Bhaskar N, Herrera ER, Soto HRL, Dameff C, Bharadia D, et al. Evaluating physical-layer ble location tracking attacks on mobile devices. In: 2022 IEEE Symposium on Security and Privacy (SP), 2022; San Francisco, CA, USA: IEEE.
58. Hasan MK, Ghazal TM, Saeed RA, Pandey B, Gohel H, Eshmawi AA, et al. A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. IET Commun. 2022;16(5):421–32.
59. Messinis S, Temenos N, Protonotarios NE, Rallis I, Kalogeras D, Doulamis N. Enhancing internet of medical things security with artificial intelligence: a comprehensive review. Comput Biol Med. 2024:108036. doi:10.1016/j.compbiomed.2024.108036.
60. Krishnendu T, Nair PP. ASLADS: a secure lightweight authentication and data transmission scheme for smart IoT devices. In: 2024 16th International Conference on COMmunication Systems & NETworkS (COMSNETS), 2024; Bengaluru, India: IEEE.
61. Qaddoori SL, Fathi la, Hammoudy MA, Ali QI. Advancing public health monitoring through secure and efficient wearable technology. Int J Saf Secur Eng. 2023;13(6):1001–14. doi:10.18280/ijsse.130603.
62. Nair G. PacketChain: a blockchain-inspired method for enhanced security of packet communication of highly constrained IoT wearable devices. In: 2023 International Conference on Control, Communication and Computing (ICCC), 2023; Thiruvananthapuram, India: IEEE.
63. Li J, Wang P, Jiao L, Yan Z, Zeng K, Yang Y. Security analysis of triangle channel-based physical layer key generation in wireless backscatter communications. IEEE Trans Inf Forensics Secur. 2022;18:948–64. doi:10.1109/TIFS.2022.3224852.
64. van Weenen E. Smart wearables in healthcare. Dimensions Intell Anal Smart Digit Health Solutions: Chapman Hall/CRC. 2024;1:23–61.
65. Ebrahimabadi M, Younis M, Lalouani W, Alshaeri A, Karimi SN. Security protocol for wearables embedded devices' data transmission. In: 2022 IEEE International Conference on E-health Networking, Application & Services (HealthCom), 2022; Genoa, Italy: IEEE.
66. Nandikotkur A. SeniorSentry: safeguarding agetech devices and sensors using contextual anomaly detection and supervised machine learning (Master's Thesis). Manipal Institute of Technology: Manipal; 2023.
67. Newaz AI, Sikder AK, Rahman MA, Uluagac AS. A survey on security and privacy issues in modern healthcare systems: attacks and defenses. ACM Trans Comput Healthcare. 2021;2(3):1–44. doi:10.1145/3453176.
68. Li J, Zhang N, Ni J, Chen J, Du R. Secure and lightweight authentication with key agreement for smart wearable systems. IEEE Internet Things J. 2020;7(8):7334–44. doi:10.1109/JIOT.2020.2984618.
69. Diaz RAC, Ghita M, Copot D, Birs IR, Muresan C, Ionescu C. Context aware control systems: an engineering applications perspective. IEEE Access. 2020;8:215550–69. doi:10.1109/ACCESS.2020.3041357.
70. Fuster J, Solera-Cotanilla S, Pérez J, Vega-Barbas M, Palacios R, Alvarez-Campana M, et al. Analysis of security and privacy issues in wearables for minors. Wirel Netw. 2023:1–17. doi:10.1007/s11276-022-03211-6.
71. Buttyan L, Holczer T. Traffic analysis attacks and countermeasures in wireless body area sensor networks. In: 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012; San Francisco, CA, USA: IEEE.
72. Barman L, Dumur A, Pyrgelis A, Hubaux J-P. Every byte matters: traffic analysis of bluetooth wearable devices. Proc ACM Interact Mo. 2021;5(2):1–45. doi:10.1145/3463512.
73. Seeam A, Ogbeh OS, Guness S, Bellekens X. Threat modeling and security issues for the internet of things. In: 2019 Conference on Next Generation Computing Applications (NextComp), 2019; Mauritius: IEEE.
74. Affia AO, Finch H, Jung W, Samori IA, Potter L, Palmer X-L. IoT health devices: exploring security risks in the connected landscape. IoT. 2023;4(2):150–82. doi:10.3390/iot4020009.

75. Ching KW, Singh MM. Wearable technology devices security and privacy vulnerability analysis. Int J Netw Secur Its Appl. 2016;8(3):19–30. doi:10.5121/ijnsa.2016.8302.
76. Classen J, Wegemer D, Patras P, Spink T, Hollick M. Anatomy of a vulnerable fitness tracking system: dissecting the fitbit cloud, app, and firmware. Proc ACM Interact Mo. 2018;2(1):1–24.
77. Meredith CMTaKA. The vulnerabilities of medical and wearable devices: tucker ellis; 2020. Available from: https://www.tuckerellis.com/publications/the-vulnerabilities-of-medical-and-wearable-devices/. [Accessed 2024].
78. Aksu H, Uluagac AS, Bentley ES. Identification of wearable devices with bluetooth. IEEE Trans Sustain Comput. 2018;6(2):221–30. doi:10.1109/TSUSC.2018.2808455.
79. Chong Y-W, Ismail W, Ko K, Lee C-Y. Energy harvesting for wearable devices: a review. IEEE Sens J. 2019;19(20):9047–62. doi:10.1109/JSEN.2019.2925638.
80. Tseng TW, Wu CT, Lai F. Threat analysis for wearable health devices and environment monitoring internet of things integration system. IEEE Access. 2019;7:144983–94. doi:10.1109/ACCESS.2019.2946081.
81. Vasilevski I, Blazhevski D, Pachovski V, Stojmenovska I. Five years later: how effective is the MAC randomization in practice? The no-at-all attack. In: ICT Innovations 2019 Big Data Processing and Mining: 11th International Conference, ICT Innovations 2019, 2019 Oct 17–19; Ohrid, North Macedonia: Springer.
82. Holliman J, Zhivich M, Khazan R, Swiston A, Telfer B. Building low-power trustworthy systems: cybersecurity considerations for real-time physiological status monitoring. In: MILCOM 2016–2016 IEEE Military Communications Conference, 2016; Baltimore, MD, USA: IEEE.
83. Vithanwattana N, Mapp G, George C. Developing a comprehensive information security framework for mHealth: a detailed analysis. J Reliable Intell Environ. 2017;3:21–39. doi:10.1007/s40860-017-0038-x.
84. Montanz Rodriguez R, Xu S. Cyber social engineering kill chain. In: International Conference on Science of Cyber Security, 2022; Matsue, Japan: Springer.
85. Exploit public-facing application: MITRE ATTACK; 2024. Available from: https://attack.mitre.org/techniques/T1190/. [Accessed 2024].
86. Jabar T, Singh MM, Al-Kadhimi AA. Mobile advanced persistent threat detection using device behavior (SHOVEL) framework. In: Proceedings of the 8th International Conference on Computational Science and Technology: ICCST 2021, 2022 Aug 28–29; Labuan, Malaysia: Springer.
87. Farooqui MNI, Arshad J, Khan MM. A layered approach to threat modeling for 5G-based systems. Electronics. 2022;11(12):1819. doi:10.3390/electronics11121819.
88. Kwon R, Ashley T, Castleberry J, Mckenzie P, Gourisetti SNG. Cyber threat dictionary using mitre att&ck matrix and nist cybersecurity framework mapping. In: 2020 Resilience Week (RWS), 2020; Salt Lake City, UT, USA: IEEE.
89. Lakshminarayana S, Praseed A, Thilagam PS. Securing the IoT application layer from an MQTT protocol perspective: challenges and research prospects. IEEE Commun Surv Tutor. 2024:1. doi:10.1109/COMST.2024.3372630.
90. Native API: MITRE ATT&CK; 2024. Available from: https://attack.mitre.org/techniques/T1575/. [Accessed 2024].
91. Command and scripting interpreter: MITRE ATT&CK; 2024. Available from: https://attack.mitre.org/techniques/T1623/. [Accessed on 2024].
92. Addo EO, Kommey B, Agbemenu AS. Wearable networks: requirements, technologies, and research trends. Int J Appl Inf Syst. 2019;12(20):1–7. doi:10.5120/ijais2019451789.
93. Karabacak F, Ogras U, Ozev S. Malicious activity detection in lightweight wearable and iot devices using signal stitching. Sensors. 2021;21(10):3408. doi:10.3390/s21103408.
94. Ahn G, Kim K, Park W, Shin D. Malicious file detection method using machine learning and interworking with MITRE ATT&CK framework. Appl Sci. 2022;12(21):10761. doi:10.3390/app122110761.

95. Subvert trust controls: MITRE ATT&CK; 2024. Available from: https://attack.mitre.org/techniques/T1632/. [Accessed 2024].
96. Hayashi VT, Ruggiero WV. Hands-free authentication for virtual assistants with trusted IoT device and machine learning. Sensors. 2022;22(4):1325. doi:10.3390/s22041325.
97. Wu H, O'Connor NE, Bruton J, Hall A, Liu M. Real-time anomaly detection for an admm-based optimal transmission frequency management system for IoT devices. Sensors. 2022;22(16):5945. doi:10.3390/s22165945.
98. Ferrag MA, Maglaras L, Derhab A, Janicke H. Authentication schemes for smart mobile devices: threat models, countermeasures, and open research issues. Telecommun Syst. 2020;73(2):317–48.
99. Kaur R, Shahrestani S, Ruan C. Security and privacy of wearable wireless sensors in healthcare: a systematic review. Comput Netw Commun. 2024:24–48. doi:10.37256/cnc.2120243852.
100. Disk wipe: disk content wipe: MITRE ATT&CK; 2024. Available from: https://attack.mitre.org/techniques/T1561/001/. [Accessed 2024].
101. López Martínez A, Gil Pérez M, Ruiz-Martínez A. A comprehensive review of the state-of-the-art on security and privacy issues in healthcare. ACM Comput Surv. 2023;55(12):1–38. doi:10.1145/3571156.
102. Papaioannou M, Karageorgou M, Mantas G, Sucasas V, Essop I, Rodriguez J, et al. A survey on security threats and countermeasures in internet of medical things (IoMT). Trans Emerg Telecomm Technol. 2022;33(6):e4049. doi:10.1002/ett.4049.
103. Besson P-V, Tong VVT, Guette G, Piolle G, Abgrall E. Ursid: using formalism to refine attack scenarios for vulnerable infrastructure deployment. arXiv preprint arXiv:230317373. 2023.
104. Zahid S, Mazhar MS, Abbas SG, Hanif Z, Hina S, Shah GA. Threat modeling in smart firefighting systems: aligning MITRE ATT&CK matrix and NIST security controls. Internet Things. 2023;22:100766. doi:10.1016/j.iot.2023.100766.
105. Rencelj Ling E, Ekstedt M. Estimating time-to-compromise for industrial control system attack techniques through vulnerability data. SN Comput Sci. 2023;4(3):318.
106. Berady A, Jaume M, Tong VVT, Guette G. PWNJUTSU: a dataset and a semantics-driven approach to retrace attack campaigns. IEEE Trans Netw Service Manag. 2022;19(4):5252–64. doi:10.1109/TNSM.2022.3183476.
107. Alamleh H, Gogarty M, Ruddell D, AlQahtani AAS. Securing the invisible thread: a comprehensive analysis of BLE tracker security in apple AirTags and samsung SmartTags. arXiv preprint arXiv:240113584. 2024.
108. Saxena P, Sharma SK. Analysis of network traffic by using packet sniffing tool: wireshark. Int J Adv Res, Ideas Innov Technol. 2017;3(6):804–8.
109. Paravathi C, Roshini D, Nayak SS. Packet sniffing. Int J Eng Manag Res. 2024;14(1):71–6.
110. Alexeevskaya YA, Molodtsova YV, Alexeevsky RA. Forensic search for traces of unauthorized access using the kerberos authentication protocol. In: 2023 International Russian Smart Industry Conference (SmartIndustryCon), 2023; Sochi, Russian Federation: IEEE.
111. Behfar MH, Di Vito D, Korhonen A, Nguyen D, Amin BM, Kurkela T, et al. Fully integrated wireless elastic wearable systems for health monitoring applications. IEEE Trans Compon, Packag Manuf Technol. 2021;11(6):1022–7. doi:10.1109/TCPMT.2021.3082647.
112. Remote services: MITRE ATT&CK; 2024. Available from: https://attack.mitre.org/techniques/T1021/. [Accessed 2024].
113. Data from local system: MITRE ATT&CK; 2024. Available from: https://attack.mitre.org/techniques/T1533/. [Accessed 2024].
114. Mills AJ, Watson RT, Pitt L, Kietzmann J. Wearing safe: physical and informational security in the age of the wearable device. Business Horizons. 2016;59(6):615–22. doi:10.1016/j.bushor.2016.08.003.

115. Wang C, Guo X, Wang Y, Chen Y, Liu B. Friend or foe? Your wearable devices reveal your personal pin. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, Xi'an, China, 2016
116. Das AK, Pathak PH, Chuah C-N, Mohapatra P. Uncovering privacy leakage in BLE network traffic of wearable fitness trackers. In: Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications, St. Augustine, FL, USA, 2016
117. Chinaei MH, Gharakheili HH, Sivaraman V. Optimal witnessing of healthcare IoT data using blockchain logging contract. IEEE Internet Things J. 2021;8(12):10117–30. doi:10.1109/JIOT.2021.3051433.
118. Song W, Jia H, Wang M, Wu Y, Xue W, Chou CT, et al. Pistis: replay attack and liveness detection for gait-based user authentication system on wearable devices using vibration. IEEE Internet Things J. 2022;10(9):8155–71. doi:10.1109/JIOT.2022.3231381.
119. Wang S, Bie R, Zhao F, Zhang N, Cheng X, Choi H-A. Security in wearable communications. IEEE Netw. 2016;30(5):61–7.
120. Guillén-Gámez FD, Mayorga-Fernández MJ. Empirical study based on the perceptions of patients and relatives about the acceptance of wearable devices to improve their health and prevent possible diseases. Mob Inf Syst. 2019;2019(1):4731048. doi:10.1155/2019/4731048.
121. Isai U, Karthikeyan G, Harideesh R. Wireless home automation communication and security with internet of things. In: 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), 2020; Vellore, India: IEEE.
122. Ioannidou I, Sklavos N. On general data protection regulation vulnerabilities and privacy issues, for wearable devices and fitness tracking applications. Cryptography. 2021;5(4):29. doi:10.3390/cryptography5040029.
123. Exfiltration over C2 channel: MITRE ATT&CK; 2024. Available from: https://attack.mitre.org/techniques/T1646/. [Accessed 2024].
124. Datta P, Namin AS, Chatterjee M. A survey of privacy concerns in wearable devices. In: 2018 IEEE International Conference on Big Data (Big Data), 2018; Seattle, WA, USA: IEEE.
125. Al-Khafajiy M, Baker T, Chalmers C, Asim M, Kolivand H, Fahim M, et al. Remote health monitoring of elderly through wearable sensors. Multimed Tools Appl. 2019;78(17):24681–706. doi:10.1007/s11042-018-7134-7.
126. Rao V, Prema K. A review on lightweight cryptography for internet-of-things based applications. J Ambient Intell Humanized Comput. 2021;12(9):8835–57. doi:10.1007/s12652-020-02672-x.
127. Kim K, Alfouzan FA, Kim H. Cyber-attack scoring model based on the offensive cybersecurity framework. Appl Sci. 2021;11(16):7738. doi:10.3390/app11167738.
128. Amro A, Gkioulos V, Katsikas S. Assessing cyber risk in cyber-physical systems using the ATT&CK framework. ACM Trans Priv Secur. 2023;26(2):1–33. doi:10.1145/3571733.
129. Hassija V, Chamola V, Bajpai BC, Zeadally S. Security issues in implantable medical devices: fact or fiction? Sustain Cities Soc. 2021;66:102552. doi:10.1016/j.scs.2020.102552.
130. Gupta A, Tripathi M, Muhuri S, Singal G, Kumar N. A secure and lightweight anonymous mutual authentication scheme for wearable devices in medical internet of things. J Inf Secur Appl. 2022;68:103259. doi:10.1016/j.jisa.2022.103259.
131. Hao Y, Tian D, Fortino G, Zhang J, Humar I. Network slicing technology in a 5G wearable network. IEEE Commun Stand Mag. 2018;2(1):66–71. doi:10.1109/MCOMSTD.2018.1700083.
132. Jan MA, Khan F, Khan R, Mastorakis S, Menon VG, Alazab M, et al. Lightweight mutual authentication and privacy-preservation scheme for intelligent wearable devices in industrial-CPS. IEEE Trans Ind Inf. 2020;17(8):5829–39. doi:10.1109/TII.2020.3043802.
133. Shi H, Zhao H, Liu Y, Gao W, Dou S-C. Systematic analysis of a military wearable device based on a multi-level fusion framework: research directions. Sensors. 2019;19(12):2651. doi:10.3390/s19122651.

134. Ajakwe SO, Nwakanma CI, Kim D-S, Lee J-M. Key wearable device technologies parameters for innovative healthcare delivery in B5G network: a review. IEEE Access. 2022;10:49956–74. doi:10.1109/ACCESS.2022.3173643.
135. Thakkar HK, Chowdhury SR, Bhoi AK, Barsocchi P. Applications of wearable technologies in healthcare: an analytical study. In: 5G IoT and edge computing for smart healthcare. Cambridge, MA, USA: Elsevier; 2022. p. 279–99.
136. Revathi S. Protocols for secure Internet of Things. Int J Educ Manag Eng. 2017;7(2):20.
137. Wang J, Hu F, Zhou Y, Liu Y, Zhang H, Liu Z. BlueDoor: breaking the secure information flow via BLE vulnerability. In: Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services, Toronto, ON, Canada, 2020; p. 286–98.
138. Ometov A, Shubina V, Klus L, Skibińska J, Saafi S, Pascacio P, et al. A survey on wearable technology: history, state-of-the-art and current challenges. Comput Netw. 2021;193:108074. doi:10.1016/j.comnet.2021.108074.
139. Sun Y, Kumar S, He S, Chen J, Shi Z. You foot the bill! Attacking NFC with passive relays. IEEE Internet Things J. 2020;8(2):1197–210. doi:10.1109/JIOT.2020.3012580.
140. Zohourian A, Dadkhah S, Neto ECP, Mahdikhani H, Danso PK, Molyneaux H, et al. IoT Zigbee device security: a comprehensive review. Internet Things. 2023:100791. doi:10.1016/j.iot.2023.100791.
141. Hireche R, Mansouri H, Pathan A-SK. Security and privacy management in internet of medical things (IoMT): a synthesis. J Cybersecur Priv. 2022;2(3):640–61. doi:10.3390/jcp2030033.
142. Kumar V, Jha RK, Jain S. NB-IoT security: a survey. Wirel Personal Commun. 2020;113:2661–708. doi:10.1007/s11277-020-07346-7.
143. Saafi S, Hosek J, Kolackova A. Enabling next-generation public safety operations with mission-critical networks and wearable applications. Sensors. 2021;21(17):5790. doi:10.3390/s21175790.
144. Al Ali J, Nasir Q, Dweiri FT. Business continuity management framework of internet of things (IoT). In: 2019 Advances in Science and Engineering Technology International Conferences (ASET), 2019; Dubai, United Arab Emirates: IEEE.
145. Zhang Q, Liang Z. Security analysis of bluetooth low energy based smart wristbands. In: 2017 2nd International Conference on Frontiers of Sensors Technologies (ICFST), 2017; Shenzhen, China: IEEE.
146. Cusack B, Antony B, Ward G, Mody S. Assessment of security vulnerabilities in wearable devices. In: Proceedings of 15th Australian Information Security Management Conference, 2017 Dec 5–6; Perth, WA, Australia: Edith Cowan University; p. 42–8.
147. Khan SA, Bajwa HR, Sundaram J, Shanmugam B. Vulnerability analysis and exploitation attacks on smart wearable devices. In: 2024 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT), 2024; Gharuan, India: IEEE.