frontiers | Frontiers in The Internet of Things

TYPE Original Research
PUBLISHED 25 November 2025
DOI 10.3389/friot.2025.1712430

OPEN ACCESS

EDITED BY
Kewei Sha,
University of North Texas, United States

REVIEWED BY
Jims Marchang,
Sheffield Hallam University, United Kingdom
Lidia Bajenaru,
National Institute for Research and Development in Informatics, Romania

*CORRESPONDENCE
Alex Akinbi,
a.akinbi@mmu.ac.uk

RECEIVED 24 September 2025
REVISED 05 November 2025
ACCEPTED 10 November 2025
PUBLISHED 25 November 2025

CITATION
Akinbi A and Raj PP (2025) A systematic security analysis of medical internet of things (MIoT) ecosystems in threat modeling scenarios. *Front. Internet Things* 4:1712430. doi: 10.3389/friot.2025.1712430

A systematic security analysis of medical internet of things (MIoT) ecosystems in threat modeling scenarios

Alex Akinbi* and Preethi Paul Raj

Department of Computing and Mathematics, Manchester Metropolitan University, Manchester, United Kingdom

The widespread adoption of Medical Internet of Things (MIoT) devices, particularly portable electrocardiogram (ECG) monitors, has accelerated since the COVID-19 pandemic, revolutionizing remote patient monitoring and healthcare delivery. However, this rapid integration has introduced significant cybersecurity challenges, especially in securing communication within the MIoT ecosystem. To address these concerns, this study presents a systematic security analysis of three popular portable ECG devices: the Beurer BM 95, KardiaMobile 6L, and OMRON Complete. The investigation begins with a structured literature review to develop a catalog of threats and a threat model specific to the devices' ecosystem. Guided by this threat model, controlled experiments were conducted to perform penetration testing and security assessments. Our findings reveal multiple security weaknesses and vulnerabilities in the Bluetooth Low Energy (BLE) implementations on these devices, exposing them to potential exploitation and attacks. Additionally, simulated attacks on paired smartphones enabled the recovery of sensitive user and patient data, highlighting further risks within the ecosystem. By uncovering these vulnerabilities, this research highlights the urgent need for stronger security measures in MIoT devices. Addressing these issues proactively is essential to enhance device resilience and protect against emerging threats in connected healthcare environments.

KEYWORDS

medical IoT, ECG, threat modeling, vulnerability analysis, penetration testing, security analysis

1 Introduction

Medical devices play a crucial role in enabling people to live more independent and healthier lives for extended periods. These devices are integral to the global and United Kingdom health and care systems, contributing significantly to the diagnosis, prevention, monitoring, treatment, and alleviation of diseases (Department of Health and Social Care, 2023). Since the COVID-19 pandemic, there has been a significant adoption in the use of Medical Internet of Things (MIoT) devices such as ventilators, infusion pumps, pacemakers, CPAP (Continuous Positive Airway Pressure) machines, blood pressure and electrocardiogram (ECG) monitors etc., for remote health monitoring and diagnosis of patients. The use of remote and ambulatory monitoring among healthcare practitioners and patients for long-term, continuous monitoring and diagnosis of cardiac diseases has since surged (Turnbull et al., 2024). In particular, the prevalence and popularity of portable cardiovascular health devices, including those capable of accurately recording single and

six-lead electrocardiograms (ECG) (Garikapati et al., 2022; Sana et al., 2020). These MIoT devices are generally affordable, portable, provide low power consumption and requirements, low cost, and provide relatively reasonable diagnostic accuracy (Turnbull et al., 2024), making them essential in medical diagnostics and the detection of heart conditions (Perez-Tirador et al., 2025) such as Atrial Fibrillation, Bradycardia, Tachycardia and Sinus rhythm with premature ventricular contractions (PVCs). These devices are mostly portable and capable of recording and transmitting patient data over short distances to other peripheral companion devices such as smartphones using protocols such as Zigbee, Bluetooth, and Z-Wave or over the internet via Wi-Fi to clinicians for analysis, review, diagnosis, or early disease detection and prevention.

Medical Internet of Things (MIoT) devices, as part of the broader IoT ecosystem, inherit common cybersecurity challenges such as device, data, and network vulnerabilities (Grispos et al., 2024; Andrea et al., 2015). Unlike smartphones and computers, MIoT devices are often resource-constrained, lacking interfaces and processing power for regular firmware updates (Hassija et al., 2019). This makes them susceptible to long-term security risks, especially since updates may require regulatory recertification, a process that varies by region and can be lengthy (Clery, 2018; Department for digital culture media and sport, 2021). Security flaws in medical devices have led to serious consequences, including injuries, misdiagnoses, and fatalities (ICIJ, 2018; Amoore, 2002; Fukami et al., 2020). High-profile recalls, such as the 2017 pacemaker incident involving nearly half a million devices, underscore the risks of poor cybersecurity (Hern, 2017). Moreover, implantable and network-integrated devices like insulin pumps and hospital telemetry systems are particularly vulnerable and attractive targets for cyberattacks (Thomasian and Adashi, 2021; Das et al., 2021).

Advanced medical technologies enhance patient care but also expand the attack surface. Cyber incidents like the WannaCry ransomware attack and the 2024 Synnovis breach demonstrate how compromised devices can disrupt hospital operations and endanger lives (Chase et al., 2022; Synnovis, 2024). Investigating MIoT-related incidents is often reactive and complex due to fragmented digital evidence, lack of forensic readiness, and architectural intricacies (Lutta et al., 2021). While resources like the MITRE–USFDA Playbook offer incident response guidance, they fall short in supporting daily risk management (Chase et al., 2022). Therefore, a proactive strategy involves threat modeling and penetration testing to identify vulnerabilities before exploitation (Jahankhani et al., 2022; Rimoli et al., 2023).

In this paper, we present a proactive approach by conducting a comprehensive and systematic security analysis of portable electrocardiogram (ECG) devices, a type of MIoT, in threat modeling scenarios. The aim is to identify potential threats and security vulnerabilities within the core MIoT architecture. By implementing this approach, we aim to highlight the importance of early detection and mitigation of risks, leading to more robust defence strategies against emerging threats that MIoT devices could introduce. This, in turn, helps improve risk management, develop robust countermeasures, foster enhanced security, privacy, and trust, and ensure the reliability and resilience of the MIoT system against cyber attacks.

The remainder of this paper is organised as follows: In Section 2, we present related works. Section 3 outlines the methodology, which includes the systematic literature review, threat modeling and attack categorization. Section 4 details the security analysis and penetration testing. Section 5 presents the vulnerability analysis and discussion of results, including key findings. In section 6, we conclude and identify future research agendas.

2 Related works

Recent studies have conducted systematic security analysis and penetration testing on several IoT systems and ecosystems and discovered several security vulnerabilities affecting the IoT landscape (Fomichev et al., 2018; Rak et al., 2022; Ficco et al., 2024; Salzillo et al., 2020). Moreover (Meneghello et al., 2019) highlighted that in various protocol implementations, such as ZigBee and BLE, convenience often takes precedence over security. The security flaws found in IoT devices, and their communication protocols are just a small part of a broader problem. IoT ecosystems, including low-cost home automation systems, are complex and decentralized. Their security depends not only on individual devices but also on the overall configuration of the entire infrastructure they are built upon (Rak et al., 2022).

Other studies have been focused more on postmortem analysis of several medical and MIoT devices in an attempt to recover evidence of forensic value (Grispos et al., 2024; Schmitt and Butterfield, 2024; Liu et al., 2023; Paratz et al., 2022). These analyses and investigations are useful in determining a timeline of events or recovering evidential data of interest post-incident (Ellouze et al., 2017). proposed a system for post-mortem analysis of lethal attack scenarios targeting cardiac implantable medical devices. Although the study proposed a formal technique for potential evidence reconstruction of forensic evidence in potential attack scenarios, they did not conduct a security analysis on any cardiac implantable medical devices to assist security analysts in identifying vulnerabilities.

Several studies have conducted penetration testing on medical devices, including insulin pumps (Li et al., 2011) and implantable devices and pacemakers (Halperin et al., 2008; Marin et al., 2016; Hei et al., 2010; Pycroft and Aziz, 2018). However, these studies did not adopt a systematic approach in the security analysis of the devices that can be adopted or followed to reproduce the testing on similar devices. Moreover, none of these studies conducted a security analysis of ECG devices (Perez-Tirador et al., 2025). analyzed the security of wearable electrocardiogram (ECG) monitoring devices against electromagnetic (EM) and power side-channel attacks. Their study showed that the success rate of the attacks varied under certain conditions and proposed mitigation. However, the study was also limited to a single threat model attack scenario.

In the study by Silva-Trujillo et al. (2023), threat modeling and network traffic analysis were performed on smartwatches by conducting passive attacks during the pairing process with companion smartphones. The findings indicated that all the smartwatches had exploitable vulnerabilities, mainly due to insecure Bluetooth Low Energy (BLE) protocol implementations. Although smartwatches record vital signals similar to ECGs, they are not classed as medical devices. Moreover, the study was limited to a

single threat model attack scenario. In the study by (Vakhter et al., 2022), they proposed a threat model and risk assessment framework for wireless biomedical devices. The study illustrated how threat modeling can be carried out or adopted by security experts, but they did not demonstrate a real-world use case of their model. Using STRIDE threat modeling (Khan et al., 2017), spoofing attacks were performed on an ECG device in the study by Cilleruelo et al. (2021).

2.1 Research gap, goals and contributions

Despite the related studies, there remains a gap in conducting a systematic security analysis and assessment based on multiple scenarios of MIoT ecosystems, particularly portable ECG devices. This analysis is essential for guiding penetration testers and security analysts during the assessment of these systems. This paper concentrates on the security analysis of portable ECG device ecosystems through threat modeling techniques. This work makes the following contributions:

- Perform a systematic literature review (SLR) to identify and classify threats and attack vectors that compromise the confidentiality, integrity, and availability of user data and MIoT device functionality;
- Collect from the SLR all threats that MIoT devices can be affected by, including ECG devices;
- Present a threat model for vulnerability analysis and assess potential security threats within portable ECG ecosystems;
- Plan and perform security analysis and penetration testing on selected portable ECG devices based on identified threats;
- Present a detailed discussion of identified vulnerabilities and associated attack vectors;
- Propose countermeasures and recommendations to enhance data protection and device security.

A systematic security analysis involves scrutinising the vulnerability of various components of the system, including software, communication links, and companion devices. For our study, we selected three popular portable electrocardiogram (ECG) devices with reasonable diagnostic accuracy: the KardiaMobile 6L six-lead ECG monitor, Omron and the Beurer M95 single-lead portable ECG devices. These portable ECG devices were chosen for this experiment because of their vital role in capturing rapid and precise heart activity and enabling remote patient monitoring. They are crucial in medical diagnostics and the detection of heart conditions such as atrial fibrillation, bradycardia, tachycardia, and sinus rhythm with premature ventricular contractions (PVCs) (Turnbull et al., 2024). Moreover, security risk assessment evaluation of telemedicine systems, such as portable ECG devices, already possesses numerous security vulnerabilities, ranging from attacks on personal and confidential data stored in the cloud to attacks on individual medical devices in close proximity to the user or patient (Kim et al., 2020).

In this study, we perform a systematic literature review, threat modeling using attack trees and penetration testing (Rimoli et al., 2023) to evaluate the security of these devices in scenarios where an attacker has access to the components and architecture of the device system. We execute possible attacks from the identified potential attack categories and report our findings.

3 Methodology

This chapter outlines the methodology adopted for conducting the security analysis of portable ECG devices. Similar to the methodology used in the systematic threat analysis of Unmanned Aerial Vehicles (UAVs) (Ficco et al., 2024), our proposed approach is based on four consecutive phases as shown in Figure 1: (i) A systematic literature review to build a threat catalogue related to MIoT systems; (ii) a system modeling phase, resulting in a semi-formal description of the MIoT system under analysis; (iii) A threat modeling phase, resulting in the categorization and visualization of the attack categories and potential attacks to portable ECG systems; (iv) A security analysis and penetration testing phase, in which attack planning and execution is performed.

3.1 MIoT system threats and threat models: systematic literature review

To achieve the objective of building a threat catalogue related to MIoT devices, we conducted a systematic literature review (SLR) under the guidance published by Kitchenham and Charters (Kitchenham and Kitchenham, 2007). The SLR relies on a three-phase process: Planning, Conducting, and Reporting. The planning phase requires formulating a research question to define the scope of reviewing the most relevant studies and answering the research question (Akinbi, MacDermott, and Ismael, 2022). The research questions to consider are as follows:

RQ1. What security threats affect MIoT systems, particularly the portable ECG device system?
RQ2. What are the methodologies to be used for producing a threat model related to MIoT systems?

3.1.1 Search strings and databases

There are several publications on the security of MIoT devices and ECG devices over the years; therefore, for this reason, we performed searches on digital libraries specified to obtain the primary studies. These criteria are necessary to get the most relevant and up-to-date resources for this research. The online digital libraries consulted include IEEE Xplore, Science Direct, ACM Digital Library, Google Scholar and Springer Link. The following search string and keywords were used for initiating the search on each online library with the Boolean operators AND/OR used as filters for the searches: *("security" OR "threats") AND ("medical devices" OR "medical IoT" OR "medical internet of things") AND ("threat modeling") AND ("medical devices" OR "medical IoT" OR "medical internet of things").* To obtain up-to-date academic sources relevant to answering the research questions, we considered publications from 1 January 2020 up to 27 January 2025; to produce the primary studies for the SLR.

3.1.2 Search inclusion and exclusion criteria

Some of the literature retrieved from the search results was found to be irrelevant and outside the scope of this study. To address this, we applied the method of inclusion and exclusion criteria, as outlined in the SLR guidelines, to filter out the irrelevant papers.

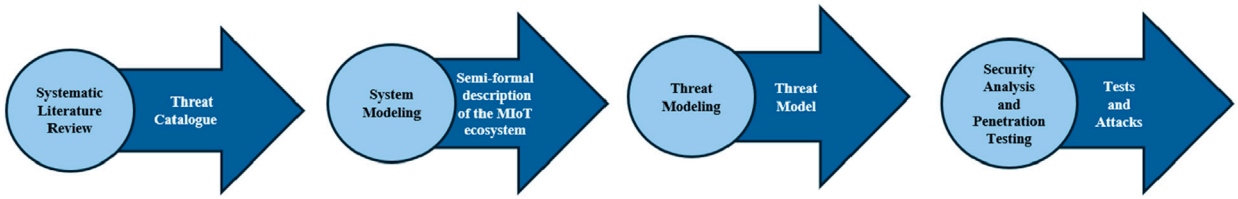

FIGURE 1
Systematic security analysis methodology (Ficco et al., 2024).

TABLE 1 Summary of SLR inclusion and exclusion criteria.

Inclusion criteria	Exclusion criteria
The paper is related to MIoT systems threats and security issues	The paper is not related to MIoT device threats and security issues
The paper is related to threat modeling for MIoT systems	The paper is not related to threat modeling for MIoT systems
The paper must be peer-reviewed	Papers that are not peer-reviewed
The paper must be written in English	Papers not written in English and duplicates of published papers
The paper must be published in a conference proceeding or a journal	Grey literature (white papers, editorial comments, book reviews, government documents and blog posts)

Table 1 outlines the inclusion and exclusion criteria used for the selection to address the research question.

3.1.3 Selection of results

The initial search across the digital libraries yielded 574 publications using specific search strings and keywords. Inclusion and exclusion criteria were applied to refine these results, resulting in the elimination of 452 publications and a reduction in the count to 57. Further filtering based on titles and abstracts excluded an additional 13 publications, leaving 44 papers. After thoroughly reading these 44 publications, reapplying the inclusion and exclusion criteria led to the removal of 10 more, resulting in a final total of 34 papers. Figure 2 shows the PRISMA flow diagram, including the number of publications selected and excluded at each stage of the selection process.

3.1.4 Results

The selected 34 publications were thoroughly reviewed, and the data extraction process is summarized in Table 2. These papers were classified to address RQ1, which aims to identify security threats to MIoT systems and RQ2, which aims to identify threat modeling methodologies used in the literature to enumerate the threats affecting MIoT systems. Most of the selected papers discussed threats and security issues related to MIoT systems and architectures, while a few specifically described security threats associated with ECG devices and their systems. We chose to extract threat attributes from the selected papers separately. As portable ECG devices are a type of MIoT device, threat attributes from the selected papers are common and closely aligned.

From the SLR results, 26 of the selected papers were either surveys describing security issues or outlining the most common threats affecting MIoT systems. A very limited number of papers focused on specific security threats related to ECG devices and their systems. Some of the selected papers provided an overview of MIoT architectures and listed the threats impacting the entire MIoT system, with a focus on compromised security requirements such as Confidentiality, Integrity, and Availability (CIA). Others adopted an attack-centric approach, detailing security threats and explaining how these threats can be executed through specific attacks. Consequently, the SLR identified 48 distinct threats associated with MIoT systems, encompassing device sensors, network communication, internal and cloud data storage, and companion devices that interact within the system. Of these 48 threats, 36 are specifically related to ECG device components and systems. We were able to map and align the threat attributes from these papers to create a comprehensive threat catalogue for portable ECG device systems in Section 3.3.

8 of the selected papers use a threat modeling approach based on a high-level description of MIoT and enumerating all the threats affecting the overall MIoT system. Previous works (Vakhter et al., 2022), described a high-level description of the primary phases of the threat modeling process that include capturing information about the system's operational environment and infrastructure, security boundaries and components, identifying assets, scenarios and attackers in order to identify threats.

The next section describes the semi-formal description of the MIoT system under analysis, in this case the portable ECG device system. We also present the threat catalog, the data model we rely on, and the attack categorization resulting from the SLR.

3.2 Portable ECG device ecosystem

The portable ECG device ecosystem helps users and patients in monitoring their heart health remotely, outside a clinical setting. Using built-in sensors, the device measures the electrical activity of the heart through skin contact or fingers and displays the data as an electrocardiogram (ECG or EKG) on a connected device like a smartphone or directly on the device itself (Bansal and Rajnish, 2018). Some integrated devices can also measure Blood Pressure level, Glucose level, Heart rate, Electrocardiogram (ECG), Electroencephalogram (EEG), Electromyography (EMG), Pulse rate, Temperature, Breathing rate, and patient's profile (Swayamsiddha and Mohanty, 2020). The measurements

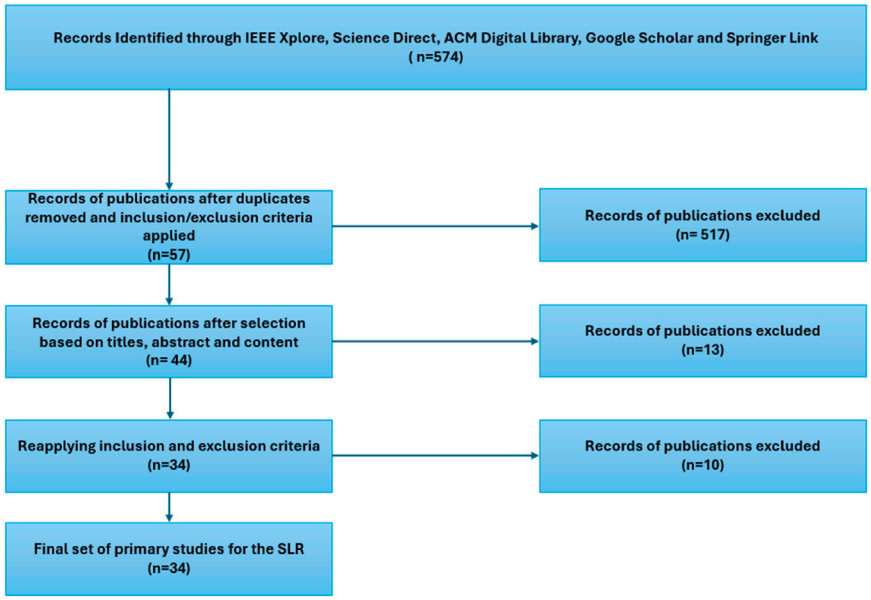

FIGURE 2
PRISMA flow diagram of the identified process for the selected 34 publications.

TABLE 2 Data extraction results.

Data extraction attribute	Number of papers	Publications
The paper is about MIoT system threats and security issues	26	Elhoseny et al., 2021; Kumar et al., 2023; Somasundaram and Thirugnanam, 2021; Kamalov et al., 2023; Bhuiyan et al., 2021; Thomasian and Adashi, 2021; Hasan et al., 2022; Hassija et al., 2021; Ghubaish et al., 2021; Papaioannou et al., 2022; Sadhu et al., 2022; Ray, Dash, and Kumar 2020; Malhotra et al., 2021; Parihar et al., 2024; Jangid, Dubey, and Chandavarkar, 2020; Perez-Tirador et al., 2025; El-Moneim et al. (2024), Rani et al., 2024; Chen et al., 2020; S. Khan et al., 2021; Karimian, Woodard, and Forte, 2020; Cilleruelo et al., 2021; Rajawat et al., 2022; Hernández-Álvarez et al., 2022; Affia et al., 2023; Newaz et al., 2021
The paper is about threat modeling for MIoT systems	8	Vakhter et al., 2022; Salayma, 2024; Alzahrani, Ahmad, and Ansari, 2022; Kwarteng and Cebe, 2023; Malamas et al., 2021

collected from the device are transmitted using Bluetooth or Bluetooth Low Energy (BLE), which are the most commonly used communication standards, to a smartphone where an app is installed to enable further data processing, aggregation, distributed storage, and display. The patient-related data can also be sent to a central cloud server for storage or directly to healthcare professionals and hospitals for continuous monitoring and analysis of the patient's physical condition (Newaz et al., 2020). The Semi-formal description of the portable ECG device ecosystem is shown in Figure 3.

3.3 Threat catalog and attack categorization

From the data extraction attributes in Section 3.1.3 of the SLR, we identified 48 distinct threats described in the selected papers. Many of these threats associated with ECG devices closely align with those related to MIoT devices. Consequently, we mapped and consolidated these threats into a single catalogue of 36 threats pertinent to portable ECG device ecosystems. Each threat was classified into an attack category based on its description and impact. Through this categorization, we identified five unique attack categories relevant to portable ECG device ecosystems. Table 3 presents a description of each attack category and its impact on the Confidentiality (C), Integrity (I) and Availability (A) of the ECG device's ecosystem.

3.4 Threat modeling

Threat modeling is a systematic approach to identifying and documenting potential threats to the device and its ecosystem. Several existing threat modeling frameworks including STRIDE, PASTA, DREAD, LINDDUN, CVSS, Attack Trees, Persona non Grata (PnG), Security Cards, Hybrid Threat Modeling Method (hTMM), Quantitative Threat Modeling Method (QTMM), Trike,

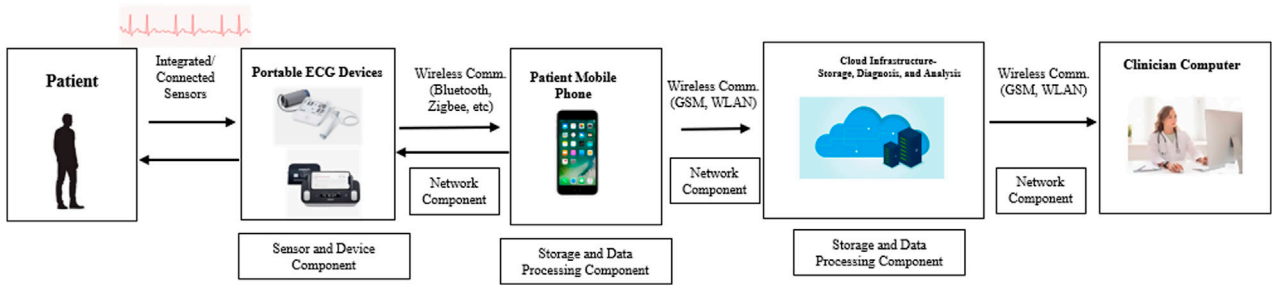

FIGURE 3
Semi-formal description of the portable ECG device ecosystem.

TABLE 3 Attack categorization of portable ECG device ecosystem threat catalog.

Threat category	Component	Attack scope	Impact	Confidentiality (C), integrity (I) and availability (A)
Companion device attacks	Smartphone, network	Gain root access to the mobile device to extract or modify ECG data	Data breach, compromised data integrity, and potential misuse of medical information	C, I
Wireless network attacks	Network	DoS attacks disrupt communication; eavesdropping and MITM attacks intercept and alter data	Service disruption, data interception, compromised confidentiality and integrity	C, I, A
Cloud/server-side attacks	Could storage and data	Breach ECG data storage via SQL injection; exploit misconfigured cloud infrastructure	Large-scale data theft, account compromise, and unauthorized access to sensitive data	C, I
Software/firmware exploitation	Device sensor, hardware, firmware	Extract hardcoded credentials; compromise OTA server to modify firmware	Unauthorized access, device malfunction, introduction of vulnerabilities or malicious code	C, I
Side channel attacks	Device, network, firmware	Power analysis and acoustic/ Electromagnetic leakage reveal sensitive information	Leakage of cryptographic keys, privacy violations, and compromised confidentiality of operations	C, I

VAST, and OCTAVE, are well summarized in (Shevchenko et al., 2018). However, threat modeling has three widely known approaches, asset-centric, attack (er)-centric, and system-centric (also named software-centric) (Khalil et al., 2024). Asset-centric threat modeling, sometimes referred to as risk assessment methods, requires knowledge of the assets within the ecosystem which is best suited with system developers. Attacker-centric threat modeling on the other hand, focuses on the attack categories that an attacker might use to compromise the ecosystem. It explores various attack paths and vulnerabilities, emphasizing how an attacker might achieve specific goals. This approach is considered more security-centric than other threat modeling approaches. Finally, the system-centric threat modeling approach maps out the entire system in diagrams and examines threats through each of the system's components.

DREAD, Trike, OCTAVE, and PASTA are well-known asset-centric threat modeling approaches (Nweke and Stephen, 2020). Attack Trees (Schneier, 1999) and Attack graphs (Potteiger et al., 2016) are attack (er)-centric approaches that combine the adversary model (knowledge, access, specificity, and resources) and the attack model (frequency, reproducibility, discoverability, functional level, asset techniques, and premise) (Khalil et al., 2024). One widely used approach for threat modeling in information systems is STRIDE (Khan et al., 2017), is categorized as both attack (er)-centric (Ucedavélez and Morana, 2015), and system-centric (Hajrić et al., 2020; Potteiger et al., 2016). STRIDE is effective in modeling security vulnerabilities in cyber-physical systems (CPS) as mentioned. However, it does not predict attack surfaces or prioritize threat modeling findings compared to Attack Trees (Mishra and Bagade, 2022; Kwarteng and Cebe, 2023). Attack trees offer a structured method for identifying threats at every system component, while STRIDE can be used to understand the entire system architecture and its components.

Attack Trees provide the benefit of identifying attribute knowledge needed for attacks, and they facilitate taking a modular approach to the attack challenge (Dewri et al., 2007; Straub, 2020). By breaking down the system into its components, Attack Trees facilitate the visualization of potential attack vectors and understanding of how different threats can compromise the system's security and data privacy.

In this paper, we utilized STRIDE to understand the threat boundaries from the components of a portable ECG device and then used Attack trees to depict potential attacks on the ECG device, illustrating various paths an attacker might take to exploit

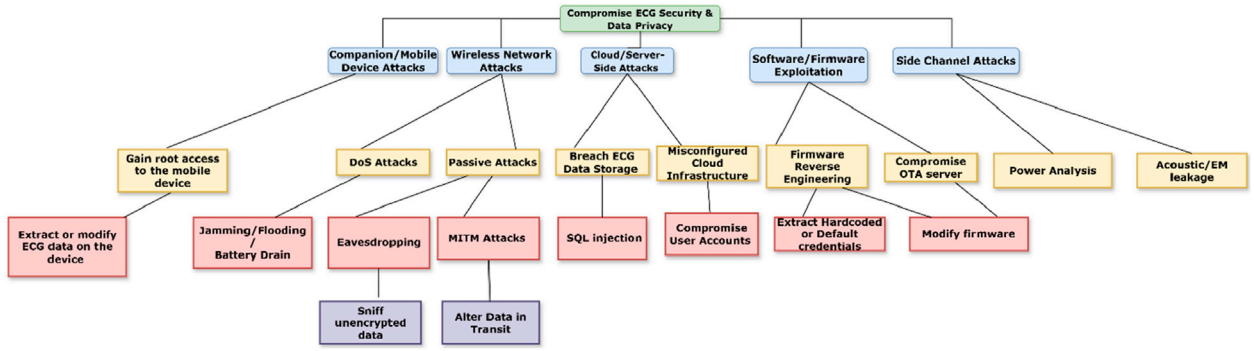

FIGURE 4
Portable ECG device attack tree.

vulnerabilities. Each node in the tree represents a potential attack, starting from the root (the main goal) and branching out into sub-goals and specific attack methods. This hierarchical structure allows for a clear visualization of how different attacks can be executed, the relationships between various threats, and the potential impact on the device's security and data privacy. At each level or branch of the attack tree, various vulnerabilities exist. Some of these vulnerabilities need to be combined to result in a breach, while others are capable of causing breaches independently (Vitkus et al., 2020). This threat model ensures a comprehensive threat identification process, enabling us to pinpoint vulnerabilities and prioritize mitigation strategies effectively.

3.4.1 ECG device ecosystem threat model using attack trees

From the threat catalogue we presented as a result of the SLR in Section 3.1, we present Figure 4, which shows the attack tree for portable ECG devices.

The attack tree diagram outlines various methods to compromise the security and data privacy of a portable ECG device. The attack tree is divided into five main categories, each representing different attack vectors. Table 1 provides a summary of the analysis of each attack vector and the implications of each one on the security and data privacy of the portable ECG device.

4 Security analysis and penetration testing

To systematically conduct a security analysis and penetration testing of the ECG device ecosystem, we conducted similar penetration tests based on our threat modeling technique in (Rak et al., 2022; Qiao et al., 2021; Ficco et al., 2024) and outlined in Section 3.3. In the subsequent sections, we present a detailed account of the experiment setup, including an outline of the discovered weaknesses, open issues and the steps involved in executing the attacks.

4.1 Ethical considerations

To generate data and simulate real-world usage, 30-s ECG recordings from several volunteers were gathered using each ECG device used in our experiments. The ethics protocol followed for the study was approved by the Research Ethics Committee of Manchester Metropolitan University, United Kingdom (REF No: 2025-72690-56619, 16th of January 2025). The participant in the data collection gave their written informed consent before enrolling in the study. The ECG recordings and measurements were anonymised to protect privacy, prevent any infringement and stored securely on the University-recommended OneDrive cloud storage.

4.2 Experiment setup and preparation

In general, an IoT ecosystem comprises numerous devices, infrastructures, services, applications, and interfaces to other applications or services (Li et al., 2019). Once we performed the attacks for each threat modeling attack category, we explored each ECG device to establish the ecosystem and environment to identify locations of potential artefacts (Salem and Hamarsheh, 2024). For the experiments, we analyzed three portable ECG devices: the Kardia Mobile 6L six-lead ECG monitor, Beurer BM 95 Upper Arm Blood Pressure Monitor with ECG Function and the OMRON Complete blood pressure and ECG monitor. Both devices feature Bluetooth Low Energy (BLE) connectivity to sync ECG readings with companion apps on a smartphone. We used a Google Pixel 8a running Android 14 as the companion smartphone, paired with each ECG device. The smartphone acts as the BLE central device, initiating outgoing connection requests to the ECG peripheral devices via the installed companion apps, and processes and stores the ECG recording data provided by the devices. A summary of the hardware specifications of all portable ECG devices in this study is presented in Table 4.

The tools used for this experiment were installed on a workstation running Windows 11, supplemented with Android rooting and BLE traffic capture capabilities. The setup included *Wireshark v 4.0.10*, a network protocol analyzer used to capture and inspect BLE traffic; *Android Debug Bridge (ADB) v 1.0.41* for device communication and file system access; *Magisk v 28.1* (Wu, 2025), a rooting tool to gain privileged access to the Android device; and *Shamiko v 1.2.1* (LSPosed, 2025), a Magisk module used to hide root status from security-sensitive mobile applications. Additionally,

TABLE 4 Summary of portable ECG devices.

ECG device	Model	Connectivity	Companion app
Beurer BM 95 Upper Arm Blood Pressure Monitor with ECG Function	BM 95	Sync via BLE	Beurer HealthManager Pro v1.15.1 Android app
AliveCor Kardia Mobile 6L six-lead ECG monitor	Mobile 6-Lead EKG	Sync via BLE	Kardia by AliveCor v4.45.0 Android app
OMRON Complete blood pressure and ECG monitor	HEM-7530T-E3	Sync via BLE	Omron Connect v7.23.1 Android app

Magnet Axiom Process v8.9.1, and *Autopsy v 4.2.1.0* were used for forensic acquisition and analysis of mobile app data and system artefacts.

The mobile applications associated with the ECG devices: Kardia, Beurer HealthManager, and OMRON Connect, were downloaded and installed on a Google Pixel 8a running Android 14. The smartphone was rooted using *Magisk* to enable full access to internal storage and app data directories. *Shamiko* was activated to bypass root detection mechanisms implemented by the ECG apps. Each ECG device was paired with the smartphone via BLE. The smartphone acted as the central device, initiating connections and receiving ECG data from the peripheral ECG devices. BLE traffic was captured as PCAP files using an *nRF52840 Dongle* in conjunction with *nRF Connect for Desktop v.4.04* and *Wireshark*, allowing inspection of BLE GATT (Generic Attribute Profile) operations and service characteristics exchanged during device communication. To identify the BLE MAC addresses of the ECG devices, a scan was initiated using the *nRF Connect* tool. Once identified, the MAC addresses were used to filter traffic in Wireshark. The BLE pairing process and data transmission sessions were recorded and analyzed to identify potential vulnerabilities or artefacts.

Privileged access to the Android file system was achieved via ADB shell commands. App-specific directories located under/data/data/<app_package_name>/were explored to extract databases, BLE logs, and cached ECG readings. Tools including *DB Browser for SQLite v 3.12.2* (Sqlitebrowser, 2016), and *Realm Studio v 15.2.1*, were used to parse and analyze SQLite and Realm databases, respectively. To ensure no conflicting processes interfered with BLE traffic capture, unnecessary services were terminated. The wireless adapter was toggled between managed and monitor modes to facilitate traffic analysis when necessary. Finally, forensic imaging of the smartphone was performed using *Magnet Axiom Process* to preserve the state of the device and its data for further offline analysis. All findings were documented, and the experiment was repeated several times across the three ECG devices to ensure accuracy, validity, consistency and reproducibility. A summary of the tools and usage is shown in Table 5.

4.3 Scope and limitations

The research examined three out of five attack categories from our threat modeling analysis: companion/mobile device attacks, wireless network attacks, and software/firmware exploitation. These categories were selected based on feasibility, ethical boundaries, and the availability of tools suitable for consumer-grade testing environments. We conducted firmware extraction on physical ECG devices, passive wireless attacks, and mobile device rooting to simulate realistic adversarial scenarios and generate data for vulnerability and forensic analysis.

However, side-channel attacks and cloud/server-side attacks were omitted due to limitations in tooling and ethical concerns, particularly regarding the handling of sensitive cloud-hosted data on third-party infrastructure. While these exclusions were necessary, they significantly constrain the generalizability of our findings. The potential impact of these untested categories is high, especially in integrated healthcare ecosystems where devices interface with cloud platforms, hospital networks, and third-party analytics services. Their omission means that the current research does not fully capture the systemic vulnerabilities that could arise in a real-world deployment. The use of consumer-grade tools and devices reflects realistic attacker capabilities, especially those of non-state actors or opportunistic adversaries. Future research would aim to incorporate side-channel and cloud/server-side attack vectors. This would require access to clinical-grade hardware, ethical clearance for cloud data analysis, and collaboration with healthcare providers to simulate realistic deployment environments.

5 Results and discussion

5.1 Firmware extraction and analysis

In our experiments, we were limited to examining the internal device components of both the Beurer BM 95 and the OMRON Complete blood pressure and ECG monitor devices. After inspecting the circuit board and the component markings, we identified the memory chip for both devices as the SST26VF032B, a 32 Mb 2.3–3.6 V Serial Quad I/O (SQI) Flash memory. Using a CH341A programmer, we connected it to the chip and extracted the stored device firmware, which we saved as a. bin file. Upon inspection, we found that the data was encrypted using OpenPGP encryption. Unfortunately, we were unable to decrypt the recovered data without knowledge of the encryption key.

5.2 Passive attack: network traffic analysis

In our experiments, we captured BLE network traffic between all three portable ECG devices (Kardia 6L, Beurer BM 95 and Omron ECG devices) that used BLE communication to synchronise ECG recording measurements with the Android smartphone using two methods.

Method 1: On the Google Pixel 8a, the BLE communication logs are stored in the file path*/data/misc/bluetooth/logs/btsnoop_hci.log*. The method we employed was to enable Bluetooth HCI (Host Controller Interface) snoop log on the smartphone and use ADB

TABLE 5 Summary of tools and usage.

Name	Purpose	Type
nRF52840 Dongle	Bluetooth Low Energy (BLE) sniffer	Hardware
CH341A Programmer v1.34	Tool used for programming and reading EEPROMs and SPI memory flash	Hardware
Android Debug Bridge (ADB) v 1.0.41	Access the Android file system to extract app data and logs	Software
Magisk v 28.1	Rooting tool for privileged access to the Android OS and file system	Software
Shamiko v 1.2.1	Hides root status from ECG mobile apps	Software
Magnet Axiom Process	Commercial forensic suite for mobile device acquisition and analysis	Software
Realm Studio v 15.2.1	Realm Databases used by mobile apps	Software
DB Browser for SQLite	SQLite database analyzer	Software
Wireshark v 4.0.10	Network protocol analyzer used to capture and inspect data packets	Software

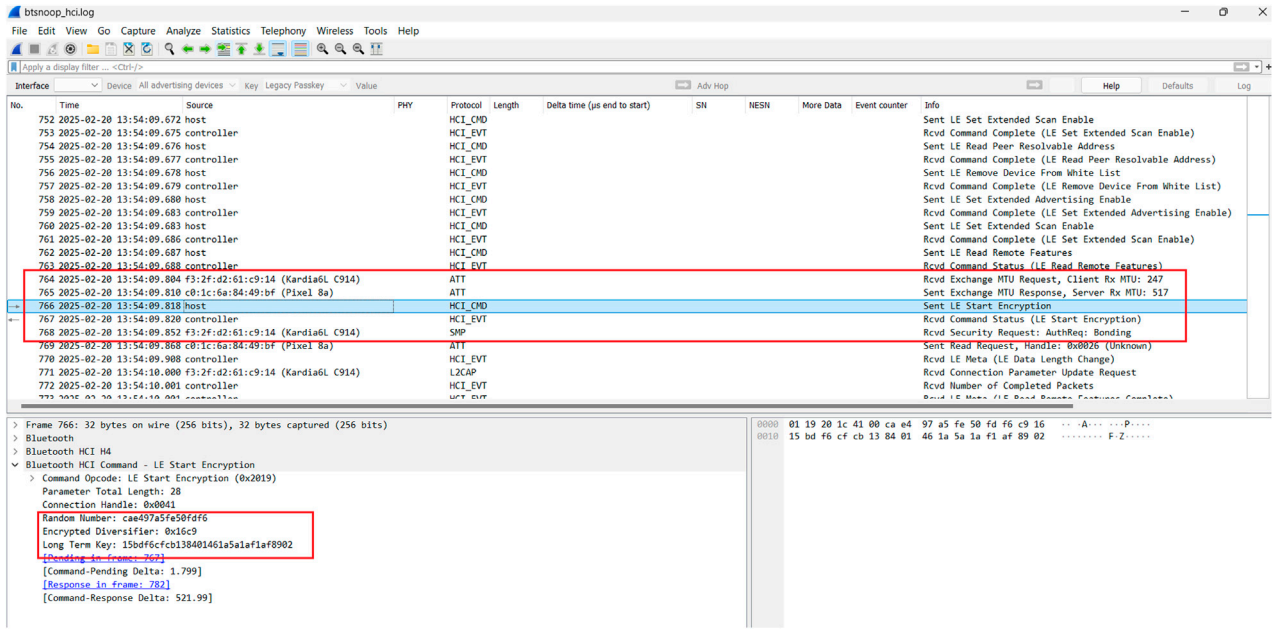

FIGURE 5
AliveCor (Kardia and Omron ECG devices) encrypted BLE communication analysis.

to retrieve the log file stored on the smartphone's file system. An HCI snoop log is a comprehensive record of all interactions between an Android device's operating system and its Bluetooth hardware controller. It captures low-level details such as commands issued, events received, and the data linked to those events (Silva-Trujillo et al., 2023).

Method 1 analysis: From our analysis of the *btsnoop_hci.log* file using Wireshark, we discovered that each device managed BLE communication using different BLE pairing methods for privacy and security. The Kardia 6L and Omron devices appeared to utilise the Long Term Key (LTK), a secret key shared and stored by both connected devices. This key, generated during the pairing process, is used to create a unique keystream for encrypting and decrypting data transmitted over the network. In Figure 5, we can see the initial MTU requests between the devices in packets 764 and 765, followed by the pairing and use of encryption in packets 766 and 767, respectively. The "*Sent LE Start Encryption*" is a command used in Bluetooth Low Energy (BLE) to initiate encryption on a connection. When a device sends the LE Start Encryption command, it includes the Long Term Key (LTK), Encrypted Diversifier (EDIV), and Random Number (Rand) to the peer device (Hlapisi, 2023). These elements are used to generate the session key for encryption. We can also see the ECG device and smartphone begin the pairing/bonding in packet 768. Hence, the network communication appeared encrypted from our analysis and is not vulnerable to MITM attacks.

However, the Beurer BM 95 device appeared to use the Just Works BLE association model, which is susceptible to MITM

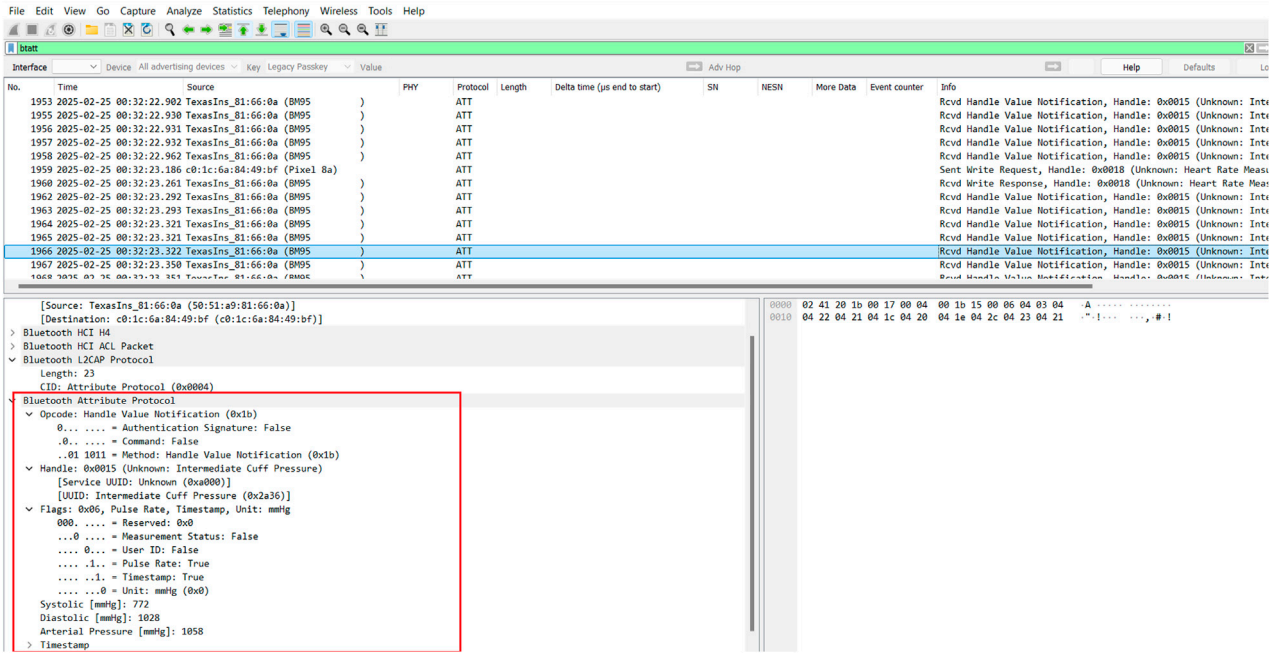

FIGURE 6
Unencrypted BLE communication sent from Beurer BM95 ECG device.

attacks. From the analysis, all BLE communication, including ECG recording measurements and blood pressure measurements sent from the Beuer 95 device, were not encrypted. Filtering the Attribute Protocol (ATT) from the log file in Wireshark, we can see the attributes and values that include blood pressure and heart rate measurements sent over the BLE network communication, as shown and highlighted in packet 1966 in Figure 6.

Method 2: It is possible to read and decode a BLE communication using dedicated hardware such by intercepting BLE network traffic (Cope et al., 2017). In our experiment, we set up the nRF52840 Dongle supported by the nRF Connect for Desktop v4.04 and configured Wireshark to capture and analyse BLE network traffic. The network capture was saved as . *pcapng* files and included BLE communication during the synchronisation of the ECG readings from all devices to the smartphone.

Method 2 analysis: From our analysis, the Kardia and Omron ECG devices appear to implement the BLE Security Mode 1, Security Level 2 involves encryption with unauthenticated pairing using Just Works due to a lack of I/O input and low computational power on the ECG devices. Although this BLE pairing method provides no Man-in-the-Middle protection (Padgette and Scarfone, 2011), the Security Level 2 implementation provides secure communication and encryption of the connection using the keys exchanged during pairing with the generation of a secret symmetric key, also known as the Long Term Key (LTK) for encryption (Lacava et al., 2022) as shown in Figure 7. After pairing, the LTK is stored in both devices, allowing for secure reconnection without repeating the pairing process, as described in our Method 1 analysis. An *LL_ENC_REQ* packet (Link Layer Encryption Request) opcode is used to initiate the encryption process between the ECG device and the smartphone. This is then followed by the *LL_START_ENC_REQ* packet (Link Layer Start Encryption Request), which signals that the devices should begin using the encryption keys for their communication, as shown in Figure 8. This step ensures that all subsequent data packets are encrypted, providing security for the data being transmitted. However, in specific scenarios, it is possible to decrypt an encrypted BLE traffic session with the knowledge of the LTK from a network capture that includes the pairing and bonding packets using BLE cracking tools such as *Crackle* (Ryan, 2025).

Our analysis of the BLE network communication between the Beurer ECG device and the Android smartphone similarly showed that no secure pairing or bonding association is implemented. The device adopts Security Mode 1, Security Level 1 BLE implementation. An analysis of the network traffic revealed that ECG and blood pressure measurements are transmitted unencrypted over the network and can be interpreted. Moreover, more sophisticated Man-in-the-Middle (MITM) attacks and Secure Simple Pairing Attacks can be conducted in specific scenarios to inject malicious readings since there is no secure pairing method implemented between both devices (Cäsar et al., 2022; Padgette and Scarfone, 2011). For example, as shown in Figure 9, we can see from the packet capture in Frame 4,606, that the ATT protocol attributes and notifications sent between the Beurer ECG device and smartphone include details of the user's blood pressure measurements, status and user ID.

In Figure 10, we can also see from the packet capture, the opcode write request in Frame 4,637 that is used by the GATT (Generic Attribute Profile) from the ECG device to write ECG recordings (heart rate measurement) to the smartphone and the subsequent acknowledgement response in Frame 4,640 both sent in plaintext.

Through our analysis, we showed that the BLE implementation mechanisms of the portable ECG devices varied, including known

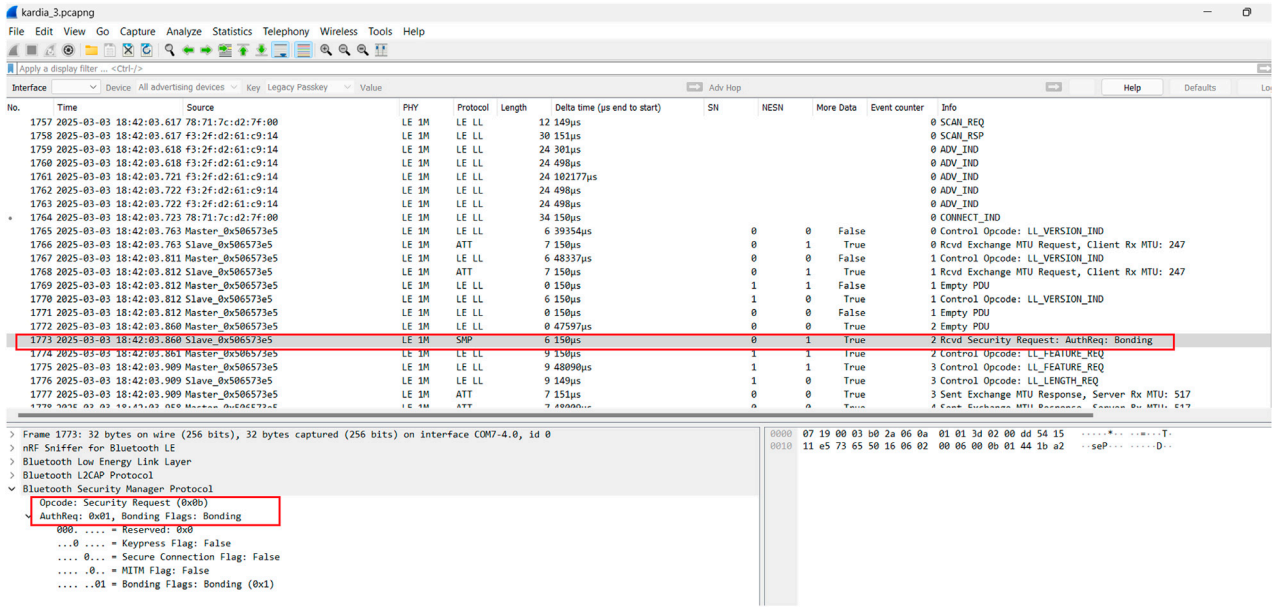

FIGURE 7
Secure BLE pairing between Kardia ECG device and Android smartphone.

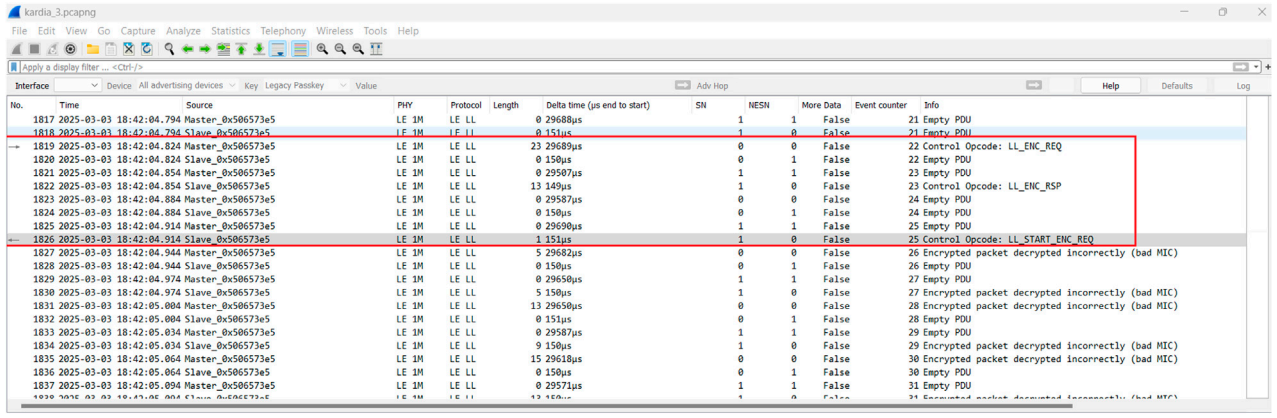

FIGURE 8
Secure BLE communication between Kardia ECG device and the Android smartphone.

weaknesses and potential attacks. We were also able to determine the BLE version for each device by analyzing the LMP version information within the HCI logs in Wireshark. Table 6 provides a summary of BLE features of the analyzed devices and open issues, including identified vulnerabilities (CVEs), Common Vulnerability Scoring System (CVSS) score, potential attacks and countermeasures.

5.2.1 Key findings

This section provides comprehensive details about the identified vulnerabilities, potential attacks, impact and related countermeasures from our network traffic analysis of the portable ECG devices.

5.2.1.1 Offline brute-force attack on legacy pairing

The legacy pairing method used in the initial BLE specifications (versions 4.0 and 4.1) was found to be vulnerable to offline brute-force attacks (Cäsar et al., 2022; Ryan, 2013). This implies that attackers could potentially exploit this weakness to gain unauthorized access by systematically guessing the pairing code. Both the Buerer BM95 and Omron ECG devices utilise BLE 4.0 and 4.1, respectively, and also use the legacy just-works pairing mode, where the passkey is fixed at 0. Therefore, an offline brute-force attack may not be necessary. In BLE Just Works legacy pairing, which falls under security mode 1 level 1 used by the Buerer BM95 device, no passkey is involved as there is no authentication

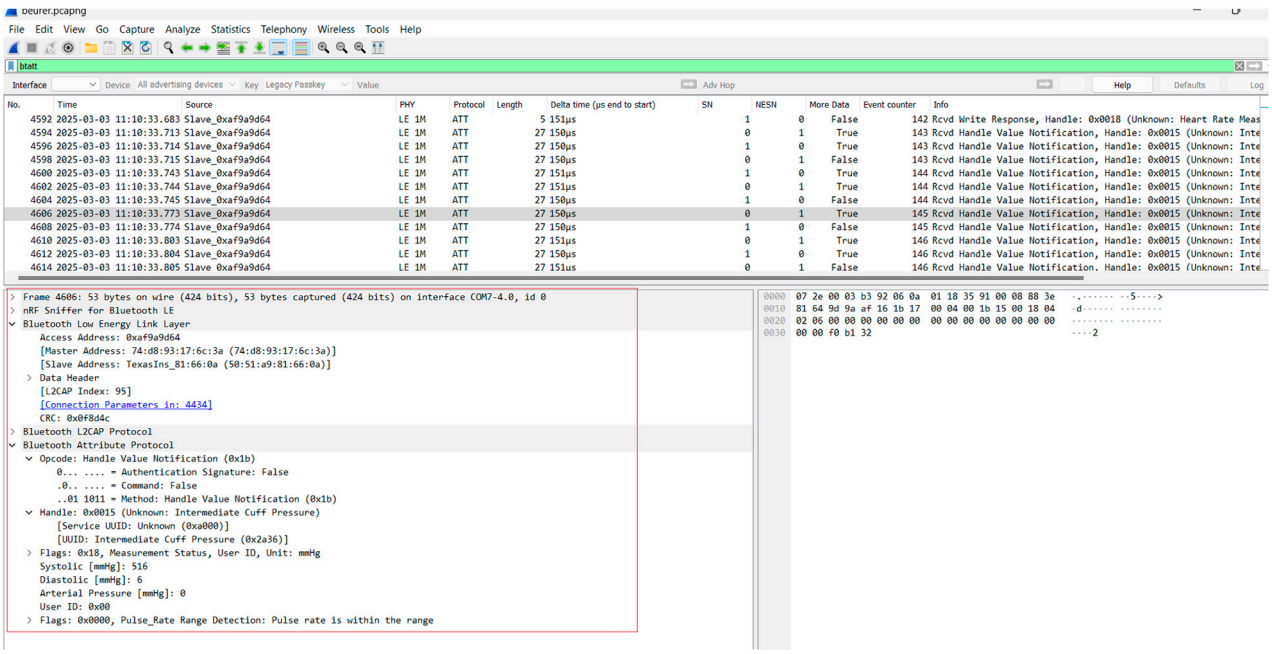

FIGURE 9
Blood Pressure health data sent unencrypted over BLE communication.

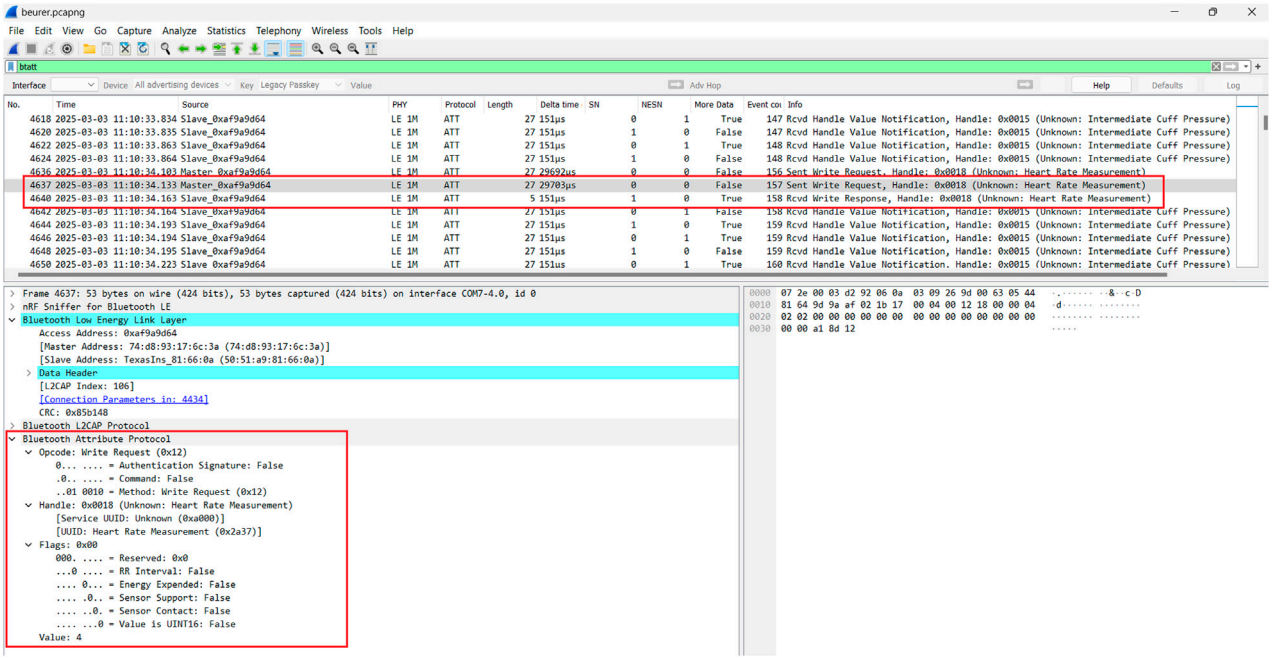

FIGURE 10
Heart rate measurements health data sent unencrypted over BLE communication.

TABLE 6 Summary of vulnerabilities and open issues.

Device name	BLE pairing methods	Pairing association model	Security mode	Level	Security description	BLE version	Vulnerability (CVE)	CVSS	Threats and attacks	Related countermeasures
Beurer BM 95 Upper Arm Blood Pressure Monitor with ECG Function	LE Legacy Pairing	Just Works	1	1	No Security (No Encryption and No Authentication)	4.0	CVE-2023-24023 CVE-2019-9506	Medium High	MITM Attacks, Replay Attacks, Eavesdropping on plaintext, Identity Tracking Possible Attacks affecting version 4.0- Offline brute force attack, KNOB attacks, BlueMirror (Cäsar et al., 2022; Claverie and Esteves 2021) attacks, BLESA spoofing	Implement Security Level 4, which uses LE Secure Connections with Elliptic Curve Diffie-Hellman for key exchange
AliveCor Kardia Mobile 6L six-lead ECG monitor	LE Legacy Pairing	Just Works	1	2	Unauthenticated pairing with encryption	4.2	CVE-2019-9506	High	MITM Attacks, Replay Attacks, Eavesdropping on encrypted data Possible Attacks affecting BLE version 4.0: KNOB attacks, BlueMirror Attack (Cäsar et al., 2022; Claverie and Esteves, 2021)	-Implement Security Mode 1, Level 4, which uses LE Secure Connections with Elliptic Curve Diffie-Hellman for key exchange -Implement version BLE 5.1 (Cäsar et al., 2022)
OMRON Complete blood pressure and ECG monitor	LE Legacy Pairing	Just Works	1	2	Unauthenticated pairing with encryption	4.1	CVE-2019-9506	High	MITM Attacks, Replay Attacks, Eavesdropping on encrypted data Possible Attacks affecting version 4.1- Offline brute force attack, KNOB attacks (Antonioli, Tippenhauer, and Rasmussen, 2020), BlueMirror (Cäsar et al., 2022; Claverie and Esteves, 2021)	Implement Security Level 4, which uses LE Secure Connections with Elliptic Curve Diffie-Hellman for key exchange

10.3389/friot.2025.1712430

or encryption. Consequently, an attacker can eavesdrop during the pairing process and compromise the LTK for security mode 1 level 2, used by the Omron ECG device used by the Omron ECG device.

CVE-2023-24023: Bluetooth BR/EDR devices with Secure Simple Pairing and Secure Connections pairing in Bluetooth Core Specification 4.2 through 5.4.

Impact: This vulnerability allows certain man-in-the-middle attacks that force a short key length and might lead to the discovery of the encryption key and live injection attacks on the ECG devices.

Related Countermeasures- The only alternative for BLE versions 4.0 and 4.1 is using the Out-of-Band (OOB) pairing mode (Cäsar et al., 2022; Renesas Electronics Corporation, 2025), to exchange pairing information securely. It is advisable to implement versions 4.2 or at least Security Level 4, which uses LE Secure Connections with Elliptic Curve Diffie-Hellman for key exchange. However, updating BLE versions is impossible on hardware devices, since they depend on the adapter integrated into the device's motherboard.

5.2.1.2 Key negotiation of bluetooth (KNOB) attacks

The Key Negotiation of Bluetooth (KNOB) attack exploits a vulnerability in the Bluetooth specification that allows attackers to manipulate the LTK encryption key and session key (SK) negotiation process. This attack can force devices to use encryption keys with only 1 byte of entropy, making them easy to brute-force ass described in the work by (Antonioli et al., 2020).

CVE-2019-9506: This vulnerability affects BLE Legacy Security (Bluetooth 4.0 and 4.1). The threats posed by the KNOB attack.

Impact: This vulnerability can cause significant disruptions in environments where BLE is a crucial component of several IoT applications (Lacava et al., 2022), including the portable ECG devices tested in our experiments.

Related Countermeasures- One effective countermeasure is to increase the minimum key length used during the encryption key negotiation process. By ensuring that the keys have higher entropy, the difficulty of brute-forcing the keys is significantly increased (Antonioli et al., 2020). Implementing stronger authentication protocols that do not rely solely on the negotiated key can provide an additional layer of security.

5.2.1.3 Blue mirror attacks

BlueMirror attacks exploit vulnerabilities in Bluetooth Low Energy (BLE) devices by mirroring legitimate device responses to trick the system into accepting unauthorized commands (Claverie and Esteves, 2021).

Impact: This can lead to unauthorized access and control over the device.

Related Countermeasures- Implementing strong authentication mechanisms, such as pairing with secure keys and using BLE Secure Connections, can mitigate BlueMirror attacks. Regular firmware updates and security patches also help in addressing known vulnerabilities.

5.2.1.4 MITM and eavesdropping attacks

MITM and eavesdropping attacks occur when an attacker intercepts and potentially alters the communication between two BLE devices.

Impact: This can lead to data breaches, unauthorized access, and manipulation of transmitted data. The portable ECG devices in our analysis all implement *Justworks,* which does not provide any protection against MITM attacks.

Related Countermeasures- Using BLE's built-in encryption and authentication features, such as LE Secure Connections, can prevent these attacks. Additionally, implementing mutual authentication and regularly updating device firmware can enhance security. Moreover, the LE secure connection pairing association models, including Numeric Comparison, Passkey Entry and out-of-band (OOB), all protect against MITM and eavesdropping attacks.

5.2.1.5 Replay attacks

Replay attacks involve capturing and retransmitting valid data packets to trick the BLE device into performing unauthorized actions.

Impact: This can lead to repeated execution of commands or unauthorized access.

Related Countermeasures- Implementing LE Secure association pairing uses nonces (randomly generated numbers used only once) and timestamps in BLE communication ensures that each data packet is unique and time-sensitive. This prevents attackers from successfully replaying captured packets. During this LE Secure association pairing between the portable ECG devices and smartphone, the devices select a freshly generated random number in order to prevent replay attacks.

5.3 Smartphone app analysis

The analysis described below is aimed at showing user data that can be recovered or exploited if an attacker is able to gain root access using malware on the user's smartphone paired with the portable ECG device. This demonstrates attacks against paired devices within the ECG device ecosystem as described in Sections 3.2, 3.3.

Kardia app analysis: The Kardia app is a mobile application that converts ECG recordings and measurements from the Kardia ECG device and presents the analysed data to the user on a GUI on the smartphone. In our experiment, we downloaded, installed, and configured the Kardia app v4.45.0 Android app (current version at the time of writing) on the Google Pixel 8a smartphone running Android 14. Once the ECG device has been paired, the ECG recordings are transferred via BLE communication and synced with the mobile app in real time. The Kardia app would not run on the rooted Android device and required the use of Shamiko v 1.2.1 (LSPosed, 2025), a module compatible with Magisk, to conceal the Android device's rooted status from the app to enable it to run successfully.

The Kardia app stores several artefacts of forensic interest in two (2) locations on the Android file system. The *common_data.db* is an SQLite database containing records of ECG measurements and the paired ECG device, and it is located in the *data/data/com.alivecor.aliveecg/databases* directory. From our findings, only 2 out of these 10 tables contain information of forensic interest, namely, *ekg* and *paired_device*. The *ekg* table contains information associated with each ECG result, indicating whether it is normal or abnormal. The table also stores the time and date for each recording associated with a user, the serial number of the paired ECG device,

TABLE 7 Summary of app-level risks on rooted Android devices.

Portable ECG android app	Runs on a rooted android smartphone	Risk severity
Kardia app v4.45.0	No	Low/High (if bypassed)
Omron Connect v7.23.1	Yes	High
Beurer HealthManager Pro v1.15.1	Yes	High

the date of the recording and the measurement of the user's heart rate in beats per minute (BPM). The*/data/data/com/alivecor.aliveecg/files/ecgs directory* incudes proprietary. *atc extension files* that can be parsed to visualize each six-lead ECG waveforms of the user stored within the app.

Omron Connect app analysis: The Omron Connect app runs on the rooted smartphone with no issues and stores generated ECG images in the*/data/data/com.omoronhealthcare.Omronconnect/files/ecgs* directory on the Android file system. The Omoron ECG device software is powered by Alivcor, the same device manufacturer as the Kardia ECG device. Therefore, ECG images are stored as. atc file formats and can be parsed to visualize the stored ECG waveforms.

Beurer Health Manager Pro app analysis: The Beurer health manager app runs on the rooted smartphone with no issues and stores artef acts in the*/data/data/com.beurer.healthmanager/files* on the Android file system. The most crucial evidential data of forensic interest are stored in Realm open-source object database management system files (Realm, 2025). In our experiments, the realm database files for each ECG recording are stored using a unique hex-encoded user-id *(e.g., user-b4bf2a1f-7d08-43d7-8b59-eb51e1b40c22. realm)* file name.

5.3.1 Key findings

This section provides the key findings, including the security weaknesses, impact and related countermeasures from our smartphone app analysis on the rooted Android smartphone. A summary of each app-level risk is presented in Table 7.

- *Security weaknesses and impact:* If an attacker gains root access to a smartphone paired with portable ECG devices, they can exploit vulnerabilities in health apps to extract sensitive user data. The *Kardia app*, although designed to block rooted devices, can be bypassed using modules like Shamiko, exposing ECG results, timestamps, heart rate, and device serial numbers. The *Omron Connect and Beurer Health Manager Pro apps* run without root restrictions, allowing access to ECG waveform files and Realm databases containing identifiable user health records. These vulnerabilities pose serious risks to user privacy, enabling unauthorized profiling and data misuse.
- *Recommended countermeasures:* Developers should integrate multi-layered root detection mechanisms to prevent app execution on compromised devices and reduce the risk of unauthorized data access. All health-related data, including databases and proprietary files, should be encrypted using robust algorithms like AES. Encryption keys must be securely stored using Android Keystore to prevent extraction by malicious actors.

6 Conclusion and future work

This paper provides a systematic security assessment of three widely used portable ECG devices, focusing on identifying vulnerabilities within their IoT ecosystems. Using structured threat assessment methods, including attack tree analysis and penetration testing, we identified exploitable flaws in Bluetooth Low Energy (BLE) protocols and Android-based companion apps. The known vulnerabilities identified are under the identifiers CVE-2023-24023 and CVE-2019-9506 with CVSS scores of medium and high, respectively. Exploiting these vulnerabilities could have significant consequences, potentially altering the behavior of the ECG devices and the manipulation of patient data in nefarious ways. Table 6 summarises the vulnerabilities we identified and the respective countermeasures. Table 7 summarized the app-level risks on rooted Android devices and user data that can be accessed if exploited. The results from this study highlight the urgent need for stronger security implementation to protect sensitive medical data and ensure reliable device operation. Although security vulnerabilities were found across all three devices, the Beurer BM95 presents a significantly higher risk compared to the KardiaMobile 6L and Omron Connect ECG devices. This is primarily due to its transmission of user data over the network without encryption, making it more susceptible to interception. Additionally, two known CVE vulnerabilities were identified in the Beurer BM95, whereas the other devices each had only one.

While the study offers valuable insights, it does not cover the entire threat landscape as outlined in the scope and limitations. Notably, side-channel and cloud/server-side attacks were excluded due to ethical and technical constraints. These areas are crucial in real-world healthcare deployments where devices interact with cloud services and hospital networks. Future research will aim to include these attack vectors, which will require clinical-grade hardware, ethical approval, and collaboration with healthcare providers to simulate realistic environments. Furthermore, future research agendas will also explore the application of emerging technologies, including machine learning and artificial intelligence, for threat detection and anomaly detection within MIoT ecosystems.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Ethics statement

The studies involving humans were approved by the Research Ethics Committee of Manchester Metropolitan University, UK (REF No: 2025-72690-56619, 16th of January 2025). The studies were conducted in accordance with the local legislation and institutional requirements. The participants provided their written informed consent to participate in this study.

Author contributions

AA: Conceptualization, Data curation, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review and editing. PR: Data curation, Investigation, Writing – original draft.

Funding

The authors declare that financial support was received for the research and/or publication of this article. This work was funded by the Faculty of Science and Engineering, Manchester Metropolitan University, United Kingdom, Research Accelerator Grant, Project ID: 3665496.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The authors declare that Generative AI was used in the creation of this manuscript. Generative AI was used to check the spelling and use of grammar in the preparation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

References

Affia, A. O., Finch, H., Jung, W., Abubakari Samori, I., Potter, L., and Palmer, X.-L. (2023). IoT health devices: exploring security risks in the connected landscape. *IoT* 4 (2), 150–182. doi:10.3390/iot4020009

Akinbi, A., MacDermott, Á., and Ismael, A. M. (2022). A systematic literature review of blockchain-based internet of things (IoT) forensic investigation process models. *Forensic Sci. Int. Digital Investigation* 42-43, 301470–43. doi:10.1016/j.fsidi.2022.301470

Alzahrani, F. A., Ahmad, M., and Ansari, Md T. J. (2022). Towards design and development of security assessment framework for internet of medical things. *Appl. Sci.* 12 (16), 8148. doi:10.3390/app12168148

Amoore, J. (2002). Quality improvement report: learning from adverse incidents involving medical devices. *BMJ* 325 (7358), 272–275. doi:10.1136/bmj.325.7358.272

Andrea, I., Chrysostomou, C., and George, H. (2015). "Internet of things: security vulnerabilities and challenges," in 2015 IEEE Symposium on Computers and Communication (ISCC), 2016-Febru (IEEE), 180–187. doi:10.1109/ISCC.2015.7405513

Antonioli, D., Tippenhauer, N. O., and Rasmussen, K. (2020). Key negotiation downgrade attacks on bluetooth and bluetooth low energy. *ACM Trans. Priv. Secur.* 23 (3), 1–28. doi:10.1145/3394497

Bansal, A., and Rajnish, J. (2018). Portable out-of-hospital electrocardiography: a review of current technologies. *J. Arrhythmia* 34 (2), 129–138. doi:10.1002/joa3.12035

Bhuiyan, M. N., Rahman, Md M., Billah, Md M., and Saha, D. (2021). Internet of things (IoT): a review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. *IEEE Internet Things J.* 8 (13), 10474–10498. doi:10.1109/JIOT.2021.3062630

Cäsar, M., Pawelke, T., Steffan, J., and Gabriel, T. (2022). A survey on bluetooth low energy security and privacy. *Comput. Netw.* 205 (March), 108712. doi:10.1016/j.comnet.2021.108712

Chase, M., Coley, S. C., Connolly, J., Daldos, R., and Zuk, M. (2022). Medical device cybersecurity regional incident preparedness and response playbook | MITRE. *Mitre* Available online at: https://www.mitre.org/news-insights/publication/medical-device-cybersecurity-regional-incident-preparedness-and-response.

Chen, H., Wang, J., Dong, X., and Cheng, Z. (2020). "Security design of ECG telemonitoring systems," in 2020 International Conference on Computer Engineering and Application (ICCEA) (IEEE), 707–711. doi:10.1109/ICCEA50009.2020.00154

Cilleruelo, C., Junquera-Sanchez, J., De-Marcos, L., Logghe, N., and Martinez-Herraiz, J.-J. (2021). "Security and privacy issues of data-over-sound technologies used in IoT healthcare devices," in 2021 IEEE Globecom Workshops (GC Wkshps) (IEEE), 1–6. doi:10.1109/GCWkshps52748.2021.9682007

Claverie, T., and Esteves, J. L. (2021). "BlueMirror: reflections on bluetooth pairing and provisioning protocols," in 2021 IEEE Security and Privacy Workshops (SPW) (IEEE), 339–351. doi:10.1109/SPW53761.2021.00054

Clery, D. (2018). *Could a wireless pacemaker let hackers take control of your heart.*

Cope, P., Campbell, J., and Hayajneh, T. (2017). "An investigation of bluetooth security vulnerabilities," in 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC) (IEEE), 1–7. doi:10.1109/CCWC.2017.7868416

Das, S., Siroky, G. P., Lee, S., Mehta, D., and Suri, R. (2021). Cybersecurity: the need for data and patient safety with cardiac implantable electronic devices. *Heart rhythm.* 18 (3), 473–481. doi:10.1016/j.hrthm.2020.10.009

Department for Digital, Culture, Media and Sport (2021). *New cyber laws to protect people's personal tech from hackers*. London: Press Release. Available online at: https://www.gov.uk/government/news/new-cyber-laws-to-protect-peoples-personal-tech-from-hackers.

Department of Health and Social Care (2023). "Medical technology strategy," in *Health and social care*. Available online at: https://www.gov.uk/government/publications/medical-technology-strategy/medical-technology-str.

Dewri, R., Poolsappasit, N., Ray, I., and Whitley, D. (2007). "Optimal security hardening using multi-objective optimization on attack tree models of networks," in Proceedings of the 14th ACM Conference on Computer and Communications Security (New York, NY, USA: ACM), 204–213. doi:10.1145/1315245.1315272

El-Moneim, K., El-Banby, G. M., Abou Elazm, L. A., El-Shafai, W., El-Bahnasawy, N. A., Abd El-Samie, F. E., et al. (2024). Securing internet-of-medical-things networks using cancellable ECG recognition. *Sci. Rep.* 14 (1), 10871. doi:10.1038/s41598-024-54830-2

Elhoseny, M., Thilakarathne, N. N., Alghamdi, M. I., Kumar Mahendran, R., Gardezi, A. A., Weerasinghe, H., et al. (2021). Security and privacy issues in medical internet of things: overview, countermeasures, challenges and future directions. *Sustainability* 13 (21), 11645. doi:10.3390/su132111645

Ellouze, N., Rekhis, S., Boudriga, N., and Mohamed, A. (2017). Cardiac implantable medical devices forensics: postmortem analysis of lethal attacks scenarios. *Digit. Investig.* 21 (June), 11–30. doi:10.1016/j.diin.2016.12.001

Ficco, M., Granata, D., Palmieri, F., and Rak, M. (2024). A systematic approach for threat and vulnerability analysis of unmanned aerial vehicles. *Internet Things* 26 (July), 101180. doi:10.1016/j.iot.2024.101180

Fomichev, M., Alvarez, F., Steinmetzer, D., Gardner-Stephen, P., and Hollick, M. (2018). Survey and systematization of secure device pairing. *IEEE Commun. Surv. Tutorials* 20 (1), 517–550. doi:10.1109/COMST.2017.2748278

Fukami, T., Uemura, M., and Nagao, Y. (2020). Significance of incident reports by medical doctors for organizational transparency and driving forces for patient safety. *Patient Saf. Surg.* 14 (1), 13. doi:10.1186/s13037-020-00240-y

Garikapati, K., Turnbull, S., Bennett, R. G., Campbell, T. G., Kanawati, J., Wong, M. S., et al. (2022). The role of contemporary wearable and handheld devices in the diagnosis and management of cardiac arrhythmias. *Heart, Lung Circulation* 31 (11), 1432–1449. doi:10.1016/j.hlc.2022.08.001

Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A., and Jain, R. (2021). Recent advances in the internet-of-medical-things (IoMT) systems security. *IEEE Internet Things J.* 8 (11), 8707–8718. doi:10.1109/JIOT.2020.3045653

Grispos, G., Tursi, F., and Mahoney, W. (2024). A digital forensic analysis of an electrocardiogram medical device: a first look. *WIREs Forensic Sci.* 6 (6), e1535. doi:10.1002/wfs2.1535

Hajrić, A., Smaka, T., Baraković, S., and Baraković-Husić, J. (2020). Methods, methodologies, and tools for threat modeling with case study. *Telfor J.* 12 (1), 56–61. doi:10.5937/telfor2001056H

Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., et al. (2008). "Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses," in 2008 IEEE Symposium on Security and Privacy (Sp 2008) (IEEE), 129–142. doi:10.1109/SP.2008.31

Hasan, M. K., Ghazal, T. M., Saeed, R. A., Pandey, B., Gohel, H., Eshmawi, A. ' A., et al. (2022). A review on security threats, vulnerabilities, and counter measures of 5G enabled internet-of-medical-things. *IET Commun.* 16 (5), 421–432. doi:10.1049/cmu2.12301

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., and Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. *IEEE Access* 7, 82721–82743. doi:10.1109/ACCESS.2019.2924045

Hassija, V., Chamola, V., Chandra Bajpai, B., Zeadally, S., and Zeadally, S. (2021). Security issues in implantable medical devices: fact or fiction? *Sustain. Cities Soc.* 66 (March), 102552. doi:10.1016/j.scs.2020.102552

Hei, X., Du, X., Wu, J., and Hu, F. (2010). "Defending resource depletion attacks on implantable medical devices," in 2010 IEEE Global Telecommunications Conference GLOBECOM 2010 (IEEE), 1–5. doi:10.1109/GLOCOM.2010.5685228

Hern, A. (2017). Hacking risk leads to recall of 500,000 pacemakers due to patient death fears. *Guard. Newsp.* Available online at: https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update.

Hernández-Álvarez, L., Pérez, J. J. B., Batista, F. K., and Queiruga-Dios, A. (2022). Security threats and cryptographic protocols for medical wearables. *Mathematics* 10 (6), 886. doi:10.3390/math10060886

Hlapisi, N. (2023). Securing BLE connections—an overview of the security protocol. *All About Circuits* Available online at: https://www.allaboutcircuits.com/technical-articles/securing-ble-connectionsan-overview-of-the-security-protocol/.

ICIJ (2018). Medical devices harm patients worldwide as governments fail on safety. *Implant Files*. 2018. Available online at: https://www.icij.org/investigations/implant-files/medical-devices-harm-patients-worldwide-as-governments-fail-on-safety/.

Jahankhani, H., George, G., Glisson, W. B., Cooper, P., Yaacoub, J. P. A., Noura, H. N., et al. (2022). Advanced digital forensics and anti-digital forensics for IoT systems: techniques, limitations and recommendations. *Internet Things Neth.* 19 (11), 100544–40. doi:10.1016/j.iot.2022.100544

Jangid, A., Kumar Dubey, P., and Chandavarkar, B. R. (2020). "Security issues and challenges in healthcare automated devices," in 2020 International Conference on COMmunication Systems NETworkS (COMSNETS) (IEEE), 19–23. doi:10.1109/COMSNETS48256.2020.9027291

Kamalov, F., Pourghebleh, B., Gheisari, M., Liu, Y., and Moussa, S. (2023). Internet of medical things privacy and security: challenges, solutions, and future trends from a new perspective. *Sustainability* 15 (4), 3317. doi:10.3390/su15043317

Karimian, N., Woodard, D., and Forte, D. (2020). ECG biometric: spoofing and countermeasures. *IEEE Trans. Biometrics, Behav. Identity Sci.* 2 (3), 257–270. doi:10.1109/TBIOM.2020.2992274

Khalil, S. M., Bahsi, H., and Korõtko, T. (2024). Threat modeling of industrial control systems: a systematic literature review. *Comput. Secur.* 136 (January), 103543. doi:10.1016/j.cose.2023.103543

Khan, R., McLaughlin, K., Laverty, D., and Sezer, S. (2017). "STRIDE-based threat modeling for cyber-physical systems," in 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe, ISGT-Europe 2017 - Proceedings. doi:10.1109/ISGTEurope.2017.8260283

Khan, S., Parkinson, S., Grant, L., Liu, N., and Mcguire, S. (2021). Biometric systems utilising health data from wearable devices. *ACM Comput. Surv.* 53 (4), 1–29. doi:10.1145/3400030

Kim, D.-won, Choi, J.-young, and Han, K.-hee (2020). Risk management-based security evaluation model for telemedicine systems. *BMC Med. Inf. Decis. Mak.* 20 (1), 106. doi:10.1186/s12911-020-01145-7

Kitchenham, B., and Kitchenham, B. (2007). Guidelines for performing systematic literature reviews in software engineering. *Tech. Rep.* Available online at: https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf.

Kumar, M., Kumar, A., Verma, S., Bhattacharya, P., Ghimire, D., Kim, S., et al. (2023). Healthcare internet of things (H-IoT): current trends, future prospects, applications, challenges, and security issues. *Electronics* 12 (9), 2050. doi:10.3390/electronics12092050

Kwarteng, E., and Cebe, M. (2023). "MEDICALHARM - a threat modeling designed for modern medical devices," in 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (IEEE), 1147–1156. doi:10.1109/TrustCom60117.2023.00157

Lacava, A., Zottola, V., Bonaldo, A., Cuomo, F., and Basagni, S. (2022). Securing bluetooth low energy networking: an overview of security procedures and threats. *Comput. Netw.* 211 (July), 108953. doi:10.1016/j.comnet.2022.108953

Li, C., Raghunathan, A., and Jha, N. K. (2011). "Hijacking an insulin pump: security attacks and defenses for a diabetes therapy system," in 2011 IEEE 13th International Conference on E-Health Networking, Applications and Services (IEEE), 150–156. doi:10.1109/HEALTH.2011.6026732

Li, S., Li, S., Raymond Choo, K.-K., Sun, Q., Buchanan, W. J., and Cao, J. (2019). IoT forensics: Amazon echo as a use case. *IEEE Internet Things J.* 6, 6487–6497. doi:10.1109/JIOT.2019.2906946

Liu, J., Sasaki, R., and Uehara, T. (2023). "An ontology-based framework for medical IoT forensic evidence," in 2023 IEEE 23rd International Conference on Software Quality, Reliability, and Security Companion (QRS-C) (IEEE), 863–864. doi:10.1109/QRS-C60940.2023.00124

LSPosed (2025). Shamiko v1.2.1. *Github*. Available online at: https://github.com/LSPosed/LSPosed.github.io/releases.

Lutta, P., Mohamed, S., Hassan, M., Jayawickrama, U., and Bastaki, B. B. (2021). The complexity of internet of things forensics: a state-of-the-art review. *Forensic Sci. Int. Digital Investigation* 38 (September), 301210. doi:10.1016/j.fsidi.2021.301210

Malamas, V., Chantzis, F., Dasaklis, T. K., Stergiopoulos, G., Kotzanikolaou, P., and Douligeris, C. (2021). Risk assessment methodologies for the internet of medical things: a survey and comparative appraisal. *IEEE Access* 9, 40049–40075. doi:10.1109/ACCESS.2021.3064682

Malhotra, P., Singh, Y., Anand, P., Kumar Bangotra, D., Singh, P. K., and Hong, W.-C. (2021). Internet of things: Evolution, concerns and security challenges. *Sensors* 21 (5), 1809. doi:10.3390/s21051809

Marin, E., Singelée, D., Garcia, F. D., Chothia, T., Willems, R., and Preneel, B. (2016). "On the (in)Security of the latest generation implantable cardiac defibrillators and how to secure them," in Proceedings of the 32nd Annual Conference on Computer Security Applications (New York, NY, USA: ACM), 226–236. doi:10.1145/2991079.2991094

Meneghello, F., Calore, M., Zucchetto, D., Polese, M., and Zanella, A. (2019). IoT: internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet Things J.* 6 (5), 8182–8201. doi:10.1109/JIOT.2019.2935189

Mishra, A., and Bagade, P. (2022). "Digital forensics for medical internet of things," in 2022 IEEE Globecom Workshops (GC Wkshps) (IEEE), 1074–1079. doi:10.1109/GCWkshps56602.2022.10008761

Newaz, I., Ashiqur Rahma, M., Selcuk Uluagac, A., and Sikder, A. K. (2020). "A survey on security and privacy issues in modern healthcare: attacks and defenses," in Proceedings - 2020 35th IEEE/ACM International Conference on Automated Software Engineering.

Newaz, A. I., Kumar Sikder, A., Rahman, M. A., and Selcuk Uluagac, A. (2021). A survey on security and privacy issues in modern healthcare systems. *ACM Trans. Comput. Healthc.* 2 (3), 1–44. doi:10.1145/3453176

Nweke, L. O., and Stephen, D. (2020). A review of asset-centric threat modelling approaches. *Int. J. Adv. Comput. Sci. Appl.* 11 (2). doi:10.14569/IJACSA.2020.0110201

Padgette, J., and Scarfone, K. (2011). *Guide to bluetooth security*. Gaithersburg: NIST. Available online at: http://csrc.nist.gov/publications/nistpubs/800-121-rev1/sp800-121_rev1.pdf.

Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., Rodriguez, J., et al. (2022). A survey on security threats and countermeasures in internet of medical things (IoMT). *Trans. Emerg. Telecommun. Technol.* 33 (6), e4049. doi:10.1002/ett.4049

Paratz, E. D., Block, T. J., Stub, D. A., Gerche, A.La, Kistler, P. M., Kalman, J. M., et al. (2022). Postmortem interrogation of cardiac implantable electronic devices. *JACC Clin. Electrophysiol.* 8 (3), 356–366. doi:10.1016/j.jacep.2021.10.011

Parihar, A., Prajapati, J. B., Prajapati, B. G., Trambadiya, B., Thakkar, A., and Engineer, P. (2024). Role of IOT in healthcare: applications, security privacy concerns. *Intell. Pharm.* 2 (5), 707–714. doi:10.1016/j.ipha.2024.01.003

Perez-Tirador, P., Jevtic, R., Cabezaolias, C., Romero, T., Abraham, O., and Gabriel, C. (2025). The effect of ECG data variability on side-channel attack success rate in wearable devices. *Integration* 103 (July), 102385. doi:10.1016/j.vlsi.2025.102385

Potteiger, B., Martins, G., and Koutsoukos, X. (2016). "Software and attack centric integrated threat modeling for quantitative risk assessment," in Proceedings of the Symposium and Bootcamp on the Science of Security (New York, NY, USA: ACM), 99–108. doi:10.1145/2898375.2898390

Pycroft, L., and Aziz, T. Z. (2018). Security of implantable medical devices with wireless connections: the dangers of cyber-attacks. *Expert Rev. Med. Devices* 15 (6), 403–406. doi:10.1080/17434440.2018.1483235

Qiao, L., Li, Y., Chen, D., Serikawa, S., Guizani, M., and Lv, Z. (2021). A survey on 5G/6G, AI, and robotics. *Comput. Electr. Eng.* 95 (October), 107372. doi:10.1016/j.compeleceng.2021.107372

Rajawat, A. S., Goyal, S. B., Bedi, P., Shrivastava, A., Bogdan Constantin, N., Raboaca, M. S., et al. (2022). "Security analysis for threats to patient data in the medical internet of things," in 2022 11th International Conference on System Modeling Advancement in Research Trends (SMART) (IEEE), 248–253. doi:10.1109/SMART55829.2022.10047322

Rak, M., Salzillo, G., and Granata, D. (2022). ESSecA: an automated expert system for threat modelling and penetration testing for IoT ecosystems. *Comput. Electr. Eng.* 99 (April), 107721. doi:10.1016/j.compeleceng.2022.107721

Rani, S., Kumar, S., Kataria, A., and Min, H. (2024). SmartHealth: an intelligent framework to secure IoMT service applications using machine learning. *ICT Express* 10 (2), 425–430. doi:10.1016/j.icte.2023.10.001

Ray, P. P., Dash, D., and Kumar, N. (2020). Sensors for internet of medical things: state-of-the-art, security and privacy issues, challenges and future directions. *Comput. Commun.* 160 (July), 111–131. doi:10.1016/j.comcom.2020.05.029

Realm (2025). *Realm database*. Available online at: https://realm.io/products/realm-database.

Renesas Electronics Corporation (2025). *BLE security*. Available online at: https://lpccs-docs.renesas.com/Tutorial-DA145x-BLE-Security/ble_security.html.

Rimoli, G. P., Granata, D., and Ficco, M. (2023). "Semi-automatic PenTest methodology based on threat-model: the IoT brick case study," in 2023 IEEE International Conference on Cloud Computing Technology and Science (CloudCom) (IEEE), 232–237. doi:10.1109/CloudCom59040.2023.00045

Ryan, M. (2013). *Bluetooth: with low energy comes low security*. Washington, DC: 7th USENIX Workshop on Offensive Technologies. Available online at: https://www.usenix.org/conference/woot13/workshop-program/presentation/ryan.

Ryan, M. (2025). Crackle. *Github*. Available online at: https://github.com/mikeryan/crackle.

Sadhu, P. K., Yanambaka, V. P., Ahmed, A., and Kumar, Y. (2022). Prospect of internet of medical things: a review on security requirements and solutions. *Sensors* 22 (15), 5517. doi:10.3390/s22155517

Salayma, M. (2024). Threat modelling in internet of things (IoT) environments using dynamic attack graphs. *Front. Internet Things* 3 (May), 1306465. doi:10.3389/friot.2024.1306465

Salem, Y., and Hamarsheh, M. M. N. (2024). Forensically analyzing IoT smart camera using MAoIDFF-IoT framework. *Forensic Sci. Int. Digital Investigation* 51 (December), 301829. doi:10.1016/j.fsidi.2024.301829

Salzillo, G., Rak, M., and Moretta, F. (2020). "Threat modeling based penetration testing: the open energy monitor case study," in 13th International Conference on Security of Information and Networks (New York, NY, USA: ACM), 1–8. doi:10.1145/3433174.3433181

Sana, F., Isselbacher, E. M., Singh, J. P., Kevin Heist, E., Pathik, B., and Armoundas, A. A. (2020). Wearable devices for ambulatory cardiac monitoring. *J. Am. Coll. Cardiol.* 75 (13), 1582–1592. doi:10.1016/j.jacc.2020.01.046

Schmitt, V., and Butterfield, E. (2024). Digital forensics in healthcare: an analysis of data associated with a CPAP machine. *Forensic Sci. Int. Digital Investigation* 48 (March), 301661. doi:10.1016/j.fsidi.2023.301661

Schneier, B. (1999). Attack trees. *Dr. Dobb's J.*, 1999. Available online at: https://www.schneier.com/academic/archives/1999/12/attack_trees.html.

Shevchenko, N., Chick, T. A., O'riordan, P., Patrick Scanlon, T., and Woody, C. (2018). *Threat modeling: a summary of available methods, carneige mellon university: software engineering*. Software Engineering Institute | Carnegie Mellon University. Available online at: https://insights.sei.cmu.edu/library/threat-modeling-a-summary-of-available-methods/.

Silva-Trujillo, A. G., Jacobo González González, M., Pérez, L. P. R., and García Villalba, L. J. (2023). Cybersecurity analysis of wearable devices: smartwatches passive attack. *Sensors* 23 (12), 5438. doi:10.3390/s23125438

Somasundaram, R., and Thirugnanam, M. (2021). Review of security challenges in healthcare internet of things. *Wirel. Netw.* 27 (8), 5503–5509. doi:10.1007/s11276-020-02340-0

Sqlitebrowser (2016). DB browser for SQLite. *Sqlitebrowser. Org.* Available online at: https://sqlitebrowser.org/.

Straub, J. (2020). "Modeling attack, defense and threat trees and the cyber kill chain, ATT& CK and STRIDE frameworks as blackboard architecture networks," in 2020 IEEE International Conference on Smart Cloud (SmartCloud) (IEEE), 148–153. doi:10.1109/SmartCloud49737.2020.00035

Swayamsiddha, S., and Mohanty, C. (2020). Application of cognitive internet of medical things for COVID-19 pandemic. *Diabetes Metabolic Syndrome Clin. Res. Rev.* 14 (5), 911–915. doi:10.1016/j.dsx.2020.06.014

Synnovis (2024). *Cyberattack information centre*. London: Cyberattack Information Centre. Available online at: https://www.synnovis.co.uk/cyberattack-information-centre.

Thomasian, N. M., and Adashi, E. Y. (2021). Cybersecurity in the internet of medical things. *Health Policy Technol.* 10 (3), 100549. doi:10.1016/j.hlpt.2021.100549

Turnbull, S., Garikapati, K., Bennett, R. G., Campbell, T. G., Kotake, Y., De Silva, K., et al. (2024). Accuracy of a single-lead ECG device for diagnosis of cardiac arrhythmias compared against cardiac electrophysiology study. *Heart, Lung Circulation* 33 (10), 1465–1474. doi:10.1016/j.hlc.2024.05.008

Ucedavélez, T., and Morana, M. M. (2015). *Risk centric threat modeling: process for attack simulation and threat analysis*. IEEE.

Vakhter, V., Soysal, B., Schaumont, P., and Guler, U. (2022). Threat modeling and risk analysis for miniaturized wireless biomedical devices. *IEEE Internet Things J.* 9 (15), 13338–13352. doi:10.1109/JIOT.2022.3144130

Vitkus, D., Salter, J., Goranin, N., and Čeponis, D. (2020). Method for attack tree data transformation and import into IT risk analysis expert systems. *Appl. Sci.* 10 (23), 8423. doi:10.3390/app10238423

Wu, J. (2025). Magisk. *Github*. Available online at: https://github.com/topjohnwu/Magisk.