Vokasi Unesa Bulletin of Engineering, Technology and Applied Science (VUBETA)
https://journal.unesa.ac.id/index.php/vubeta
Vol. 3, No. 2, 2026, pp. 412~438 DOI: 10.26740/vubeta.v3i2.44150
ISSN: 3064-0768

Comparative Analysis of Embedded Systems for Mobile Health Applications Against Cyber Attacks: A Review Study

Anayo Chukwu Ikegwu[1*], Excellence Essien Akparawa[2], Uzoma Rita Alo[3]
[1]Computer Science Department, Faculty of Physical Sciences, Alex Ekwueme Federal University, Ndufu-Alike, Ebonyi State, Nigeria.
[1,3]Software Engineering Department, Faculty of Natural and Applied Sciences, Veritas University Abuja, Nigeria.
[2]Computer Science Department, Faculty of Natural and Applied Sciences, Veritas University Abuja, Nigeria.

Article Info

Article history:

Received July 15, 2025
Revised December 23, 2025
Accepted April 07, 2026

Keywords:

Embedded Systems
Mobile Health Applications
Cyber Attacks
Cybersecurity
mHealth

ABSTRACT

Mobile health applications and embedded systems have transformed healthcare by offering real-time monitoring, remote diagnostics, and better patient outcomes. However, reliance on digital health solutions introduces significant cybersecurity challenges, requiring robust security measures to protect sensitive patient data. This paper discusses the security needs of embedded systems in mHealth, emphasizing the importance of confidentiality, integrity, and availability to safeguard data. It reviews compliance frameworks such as HIPAA and GDPR, which set data protection standards. The research highlights the need for cybersecurity to support patient safety, mitigate risks after device compromise, and defend against emerging threats. Comparative studies of current security technologies, both hardware- and software-based, show their impact against cyberattacks. Finally, the paper discusses trends such as AI-driven threat detection, post-quantum cryptography, and edge computing as future mHealth security paradigms. By adopting strong security protocols, healthcare institutions can boost trust, meet regulations, and secure mHealth embedded systems.

1. INTRODUCTION

The integration of embedded systems into mobile health (mHealth) applications has transformed today's healthcare, enhancing, by and large, patient-provider access to critical health information in real time. The application of wearable, remote sensing, and sensor-based health technologies has enabled continuous health monitoring alongside personalized treatment interventions [9]. As the use of mHealth solutions grows, vulnerabilities exist that cybercriminals could exploit to compromise patient privacy, data integrity, and system availability. Security for embedded systems in mHealth solutions has hence emerged as a central part of healthcare cybersecurity today. The fundamental security concerns in mHealth embedded systems revolve around the triad: confidentiality, integrity, and availability (CIA). Confidentiality safeguards sensitive health information so that it is accessed only by authorized individuals, in accordance with regulatory requirements such as HIPAA in the US and GDPR in the EU [15]. Integrity prevents data manipulation so that health records are not altered or destroyed, and availability ensures that health data are accessible when needed, preventing obstruction of patient care [30]. Addressing these issues requires a multi-layered security solution through encryption, access control, authentication, and intrusion detection. Research in 2024 and 2025 indicates that AI-based threat intelligence and zero-trust security frameworks are increasingly relevant to mHealth app security. [87] note that machine learning algorithms are increasingly used to identify anomalies in real time, thereby minimizing the likelihood of cyberattacks on patient data.

*Corresponding Author
Email: ikegwua@veritas.edu.ng

Likewise, [33] states that zero-trust architectures that require ongoing confirmation of user identity and device access have been effective in preventing unauthorized access to healthcare systems. Additionally, [41] notes that blockchain-based security systems are becoming increasingly popular for maintaining data integrity and decentralized access controls in mHealth apps. Moreover, regulatory compliance takes center stage when shaping security protocols for mHealth apps. Both healthcare professionals and mobile app developers must comply with strict data protection regulations, such as HIPAA and GDPR, to maintain legal and ethical standards for patient data management [81]. Adhering to such regulations not only reduces legal liabilities but also enhances users' confidence and trust in digital healthcare services. Additionally, mHealth security extends beyond data protection to encompass patient safety. Embedded system threats can be life-critical, for example, unauthorized access to life-sustaining medical devices that control vital functions such as insulin dosage and cardiac rhythm monitoring [66]. The paper presents a detailed analysis of embedded system security solutions for mHealth, comparing hardware- and software-based approaches for mitigating cyberattacks. A recent study by Tajudeen & Nureni (2025) examined cyberattacks by surveying threat intelligence and trust through sharing strategies. This study is based on threat intelligence (TI) classification, the associated methodologies, and ways to mitigate cybersecurity vulnerabilities. However, it does not cover embedded systems and their mobile health applications. Also, Ikegwu et al. (2025) presented a thorough systematic literature review of cyber threats and mHealthcare, covering enabling technologies, threat models, and detection mechanisms. Nonetheless, embedded systems were not discussed. Furthermore, new security technologies such as AI-driven threat detection, post-quantum cryptography, and edge computing are examined to determine how they can be leveraged to enhance the resilience of mHealth security systems. Recognizing the evolving mHealth cybersecurity landscape, healthcare organizations can adopt forward-thinking security measures that protect patient information, facilitate regulatory compliance, and enhance the stability of digital health systems.

1.1. Problem Statement

Despite the transformative potential of embedded systems in mHealth—enabling real-time monitoring, remote diagnostics, and personalized care—these systems face persistent and evolving cybersecurity threats. Key challenges include:

- Resource Constraints – Wearable and implantable mHealth devices often have limited processing power, memory, and battery life, making it difficult to implement computationally intensive security measures such as advanced encryption or AI-driven threat detection [13].
- Real-Time Processing vs. Security Overhead – The need for the instant transmission of physiological data for clinical decision-making often conflicts with the latency introduced by robust security protocols, potentially delaying critical interventions [13].
- Energy Limitations – Continuous monitoring, encryption, and authentication processes increase power consumption, reducing battery life and affecting long-term usability [13].
- Vulnerabilities from Poor Security Practices – Weak encryption, misconfigured databases, insufficient authentication, and inadequate security testing have led to major breaches in mHealth systems, exposing sensitive patient data to unauthorized access [53][70][7].
- Regulatory Compliance Challenges – Adhering to healthcare data protection laws such as HIPAA and GDPR remains difficult, especially for smaller developers or low-resource manufacturers, risking both patient trust and legal penalties [81], My Data-Trust 2022.

1.2. Contributions to Current Knowledge

- We provided a succinct explanation of embedded systems for mobile health.
- Emerging security technologies, such as AI-driven threat detection, post-quantum cryptography, and edge computing, are explored to assess their potential to enhance the resilience of mHealth security frameworks.
- We provided a deep understanding of the different cybersecurity technologies in mHealth.
- We highlighted the different attack surfaces for embedded systems.
- We then analyzed the challenges for securing embedded systems against cyberattacks.

The remaining structure of the paper is organized as follows: Section 2 discusses mobile health-specific cyber-attacks. The paper's taxonomy is shown in Figure 1.

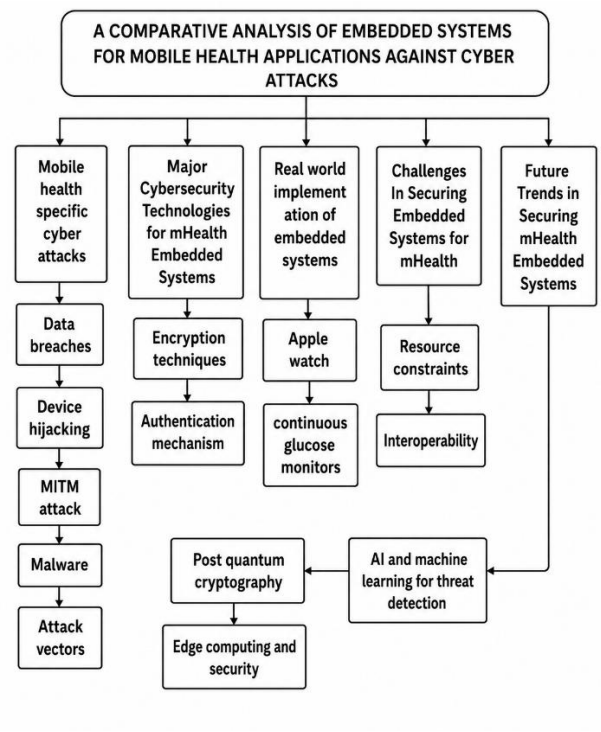

Figure 1. Taxonomy of a comparative analysis of embedded systems for mHealth applications against cyber attacks

2. MOBILE HEALTH-SPECIFIC CYBER ATTACKS

Mobile health faces distinct cyber threats, which will be discussed below. These threats exploit vulnerabilities in mobile platforms, wireless networks, and cloud storage, exposing patient data, undermining healthcare delivery, and compromising the integrity of sensitive information. Hence, it jeopardizes patient safety and confidentiality. The threats aforementioned highlight the need for robust security measures and stringent data protection policies.

2.1. Data Breaches

According to [54], a data breach is a security incident in which personal or confidential information is accessed, disclosed, or lost without the owner's permission or knowledge. The United States Department of Health and Human Services defines a data breach as “the unlawful use or disclosure of confidential health information that compromises the privacy or security of it under the privacy rule that poses a sufficient risk of financial, reputational, or other type of harm to the affected person” [84].

There are risks that stem from data exposure, some of which are financial harm that could expose victims to fraud and identity theft, or financial hardship if the victim pays a ransom, and reputation harm, especially for high-profile victims [50]. According to [94], when it comes to securing data, users of these systems should try to prevent the most likely breaches, such as leaving mobile devices unsecured, sharing passwords or leaving them written on notes, accessing sensitive information in public areas using open Wi-Fi networks, or even losing a mobile device. Reducing the potential impact of data breaches can also be achieved by avoiding storing data on mobile devices. For example, if a protocol includes developing a personal health record with detailed health data, the research team might consider encrypting the data and storing it on a secure server for aggregation. Users could access the data via a wireless network, but the data would not remain on the device after the application closed [94].

2.2. Device Hijacking

Device hijacking, or cyber hijacking, is a type of cyberattack in which an attacker takes control of computer systems, software programs, and/or network communications without the user's consent or knowledge [36]. In the space of medical devices and applications, modern technologies, such as implantable and wearable medical devices (IWMDs), biosensors, and BANs, have certainly enhanced overall healthcare systems for patients and medical professionals [69]. However, these more advanced healthcare systems are “more” complex in both software and hardware. Although the adoption of new technologies in the healthcare domain is at an early stage, several software and hardware gaps have already been identified, which could lead to malicious attacks. Open-source development platforms and continuous connectivity enable attackers to

exploit the security and privacy of healthcare systems. In recent years, several healthcare security issues have been reported both in the media and the academic community. For example, a story went viral online that doctors disabled the wireless connectivity of a former U.S. vice president's pacemaker to protect it from hacking [69].

2.3. Man in the Middle Attacks

In a MITM attack, an intermediate participant alters the messages of two legitimate participants [31]. A man-in-the-middle attack is an attack in which an attacker relays and possibly blocks communication between two parties who believe they are communicating directly with each other, without a third party present [59].

There are five classifications that identify the vulnerabilities attackers leverage to implement MITM attacks [14].

(i) Cipher Block Chaining: Block ciphers require blocks of fixed length. If the data in the last block is not a multiple of the block size, padding is added to fill the remaining space. The server ignores the padding content. It only checks if the padding length is accurate and verifies the Message Authentication Code (MAC) of the plain text. That means the server cannot verify whether anyone modified the padding. Attackers can use inherent vulnerabilities in the Cipher Block Chaining (CBC) mode of operation to decrypt the contents of an HTTPS message. (Example lucky 13 and poodle attack).

(ii) Compression: A key part of HTTPS communications is the compression of message contents to minimize resource usage. Attackers exploit message compression by comparing size differences, enabling inference of message content. (Example, crime, breach, and time attack).

(iii) Export Key: This classification applies to attacks that capitalize on export-grade security keys. These keys were initially introduced to comply with United States cryptography export regulations. The regulations limited the strength of cryptographic software, with the intention that weaker export keys could be broken by United States government agencies. However, attackers can also exploit these export-grade security keys to intercept HTTPS traffic and decrypt its contents. (Example, logiam, and freak attack).

(iv) Implementation Error: These errors are typically the result of a poorly applied security feature or a bug in the system. Attackers can capitalize on these implementation errors to launch attacks. (Example, Berserk, Komoriare director, CCS injection, drown, and Heartbleed attack).

(v) Renegotiation: Renegotiation allows HTTPS connection parameters and keys to be changed in existing connections upon request. Attackers can exploit the Renegotiation feature to establish their own connection, then splice another connection to use the attackers' connection settings. (Example, triple handshake attack and renegotiation attack). An illustration of a Man-in-the-Middle attack is shown in Figure 2.

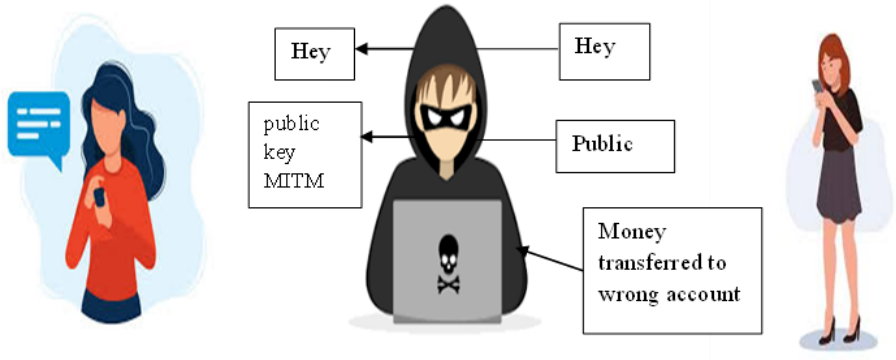

Figure 2. Man-in-the- middle attack

2.4. Malware

Any software or application that is written with malicious intent is called malware. [69]. Malware is any software used to disrupt computer operation, perform unauthorized functions, gather sensitive information, or gain access to personal information systems [18]. Malware can range from a simple nuisance, such as pop-up advertising, to an intrusion causing severe harm, such as stealing passwords and data or infecting other machines on a network. Malware appears in different forms, such as Viruses, Spyware, Adware, Nagware, Backdoors, Rootkits, Trojan horses, Botnets, keyloggers, spammers, Flooders, Zombies, Auto-Rooters, logic bombs, and Worms. On mobile platforms, malware can spread between devices via infection vectors such as Bluetooth, MMS, SMS, Internet networks, executable files, email, and web vulnerabilities [18].

Malware can be grouped by behavior and payload. They can also be grouped by the way they spread or grow [18]. There is a group that needs to be triggered by a program or by some users' activities to allow them to duplicate and spread (Such as viruses). The second group of malware (Worms) can self-duplicate and automatically scan for vulnerable victims across the internet or any medium in contact with them. The third category evolves into exploits and unknown weaknesses. They employ several attack vectors to duplicate. These last categories are known to strike faster, preventing timely intervention by security administrators [18]. Mobile devices infected with Malware are usually under the control of attackers [18]. They can provide an unapproved opening for the attacker to access and steal very personal, sensitive information such as Bank details, confidential messages, files, and photos, and to perform online/click fraud and phishing. The attacker will also be able to remotely control the device by placing unauthorized phone calls, sending spam emails, SMS, and MMS [18].

2.5. Attack Vectors in mHealth

A method by which a hacker gains unauthorized access to a private system is called an attack vector. An attack vector is usually a complex process in which threat actors gather intelligence to understand their victims, identify security weaknesses, and then attempt to gain access to the system [60]. According to [60], the attack surface is the set of all possible entry points into a system. In other words, it's the combination of all attack vectors within an IT environment and organizational network. Five connected attack surfaces are vulnerable to cyberattacks, as discussed below. Figure 3 shows the different attack vectors in mHealth.

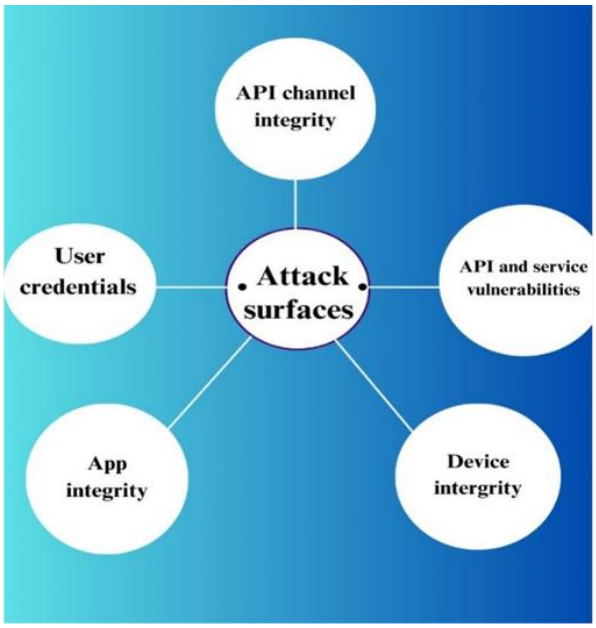

Figure 3. Attack Vectors in mHealth

(i) Attack Surface 1: User Credentials

Hackers steal information such as emails, usernames, phone numbers, IP addresses, and passwords through spoofing, phishing, and large-scale data breaches. Spoofing is when someone impersonates an authorized source to obtain private information for malicious purposes. Phishing involves sending an email that holds a harmful link or attachment that carries malware [89]. Despite the best efforts to secure the login process, hackers still bypass security protocols such as biometrics and 2-factor authentication by exploiting social engineering tricks to compromise devices and retrieve authentication codes. Another way cybercriminals steal information is by tricking users into logging in to fake applications. These apps single out popular activities such as betting and gaming.

(ii) Attack Surface 2: App Integrity

A vital characteristic of a mobile application is the integrity of its code. Hackers attacking the integrity of a mobile app seek to do three things: Draw out information they can use to launch an attack on the app's API using a different tool. Obtain identity keys to reverse engineer how the API works and exploit the API's business function. Reverse engineering is the most well-known way cybercriminals attack a mobile application [89]. Convert the application into an attack tool that redirects the user's

payments or advertising revenue to the attacker's account. To safeguard an application's integrity, developers need to determine the legitimacy of requests received by the API server. Such requests come from different sources, such as bots, automated scripts, or manual access through your API's backend [89].

(iii) Attack Surface 3: Device Integrity

Rooting/jailbreaking is a common skill used by hackers to access a gadget's pre-installed security features in the original version of the operating system. Some mobile device users root or jailbreak their devices for legal reasons. For instance, a user might want to install customized applications, while some may want to load apps unavailable in the manufacturer's app store. Despite these legal reasons, tampering with a device's integrity exposes it to attackers because its built-in security has been compromised. This vulnerability now extends to your mobile apps, as they run in an unprotected environment [89]. Another method hackers use to attack your device's integrity is tampering with its code. During runtime, they inject harmful code into the app using an instrumentation framework. These frameworks are connected to critical functions that manipulate input data, produce output results, modify user communications, or alter app behavior [89]. To protect device integrity from such attacks, implement run-time self-defense code in your mobile app. This code spots instrumentation frameworks and also recognizes rooted/jailbroken devices [89].

(iv) Attack Surface 4: API Channel Integrity

In most cases, channel integrity is at risk when the communication channel between the mobile app and the API is exposed via public Wi-Fi. This channel is the primary attack surface hacker's target. Despite using TLS/SSL to encrypt internet traffic and establish secure connections, hackers can still exploit Man-in-the-Middle (MitM) attacks between the mobile app and the API server to steal data and read API queries/responses [89]. The primary aim of MitM attacks is to hoodwink users and the servers they're communicating with. In reality, a third actor is impersonating both ends of the channel. Hackers use a MitM strategy to analyze the communication channel between a user and the API server to determine which attack strategy to use [89]. Channels that hackers research to apply MitM attacks include:

- Understanding API protocols in use to extract code to mimic legitimate traffic rhythms.
- Collecting API keys in transit to insert scripts to convince the server that the communication is coming from a genuine user interaction.
- Extracting user records or authentication tokens in transit to implant them in scripts that convince the server that the interaction is from a trusted user.
- Controlling transaction requests made through the API such that the action requested from the server is different from that initiated by the remote user.
- Exposing API weaknesses, e.g., Broken Object Level Authorization (BOLA), to exploit them to retrieve information not typically available to a given user.

To protect your channel's integrity, certificate pinning is best practice because it makes traffic interception much more difficult. A step beyond TLS, certificate pinning further locks down the connection [89]. Part of the TLS protocol requires the presentation and checking of public keys between the mobile app and the backend server or endpoint. These keys or certificates are recognized by the mobile device if they are signed by a recognized Certificate Authority (CA) and that authority is present in the device's CA trust store. Any MitM tool, such as Mitm Proxy, presents its own key to the mobile app, which is not recognized because it is not signed by a CA available in the mobile device's trust store [89]. With pinning in place, the given key must be signed by a CA in the mobile device's trust store and match one of the set of certificates encoded in the app itself. For the hacker, this means that the app needs to be altered to change the stored certificate set [89].

(v) Attack Surface 5: API and Service Vulnerabilities

There are three common goals a hacker seeks to achieve when targeting an API with an automated tool [89]: Login system attacks; attackers use brute-force techniques such as credential stuffing to test stolen credentials and their validity against the API. If they work, these credentials are employed to retrieve PI information. Data theft: Cybercriminals also deploy APIs to steal personal credentials from user accounts, including files, photos, and credit card information. Theft is carried out through data scraping, exploiting Broken Object-Level Authorization, and any other weaknesses to manipulate personal identity data. Denial-of-Service (DoS) attacks aim to render endpoints unavailable by overloading them with malicious requests, causing the mobile app to go offline.

The cyberattack methods, description, strengths, and weaknesses are presented in Table 1.

Table 1. Cyber Attack Methods, Descriptions, Strengths, and Weaknesses for mHealth Applications

Cyberattack methods	Description	Strength	Weakness	Reference
SQL Injection	Injecting malicious SQL code to manipulate or access a database.	Can expose sensitive health records.	Proper input validation and secure coding practices reduce risk.	[15]
Zero-Day Exploits	Attacks targeting previously unknown vulnerabilities before a fix is available.	Difficult to defend against due to the lack of prior knowledge.	Regular software updates and threat intelligence can help.	[29]
Ransomware	Malicious software that encrypts a victim's data, demanding payment for decryption.	Can cause severe financial and operational damage.	Backups and strong cybersecurity measures can limit impact.	[33]
Man-in-the-Middle (MITM)	An attack where an attacker intercepts and alters communication between two parties.	Can compromise data integrity and confidentiality.	Encryption protocols like TLS/SSL can prevent MITM attacks.	[41]
Denial of Service (DoS)	Overloads a system with excessive requests, making it unavailable to users.	Can disrupt critical healthcare services.	Rate limiting and DDoS protection tools can mitigate impact.	[65]
Insider Threats	Unauthorized access or malicious actions by employees or insiders.	Hard to detect as attackers often have legitimate access.	Strict access controls and monitoring can mitigate risks.	[81]
Phishing	A social engineering attack where attackers deceive users into revealing sensitive information through fake emails or websites.	Highly effective against untrained users.	Relies on user awareness and training to mitigate.	[87]

3. METHOD

This study adopted a structured literature review to investigate the security requirements and challenges of embedded systems in mobile health (mHealth) applications in the context of cyberattacks. The process involved:

Literature Identification – Peer-reviewed journal articles, conference proceedings, and authoritative technical reports from 2017 to 2025 were retrieved from reputable databases, including IEEE Xplore, SpringerLink, Elsevier, and ACM Digital Library. Search terms included embedded systems, mHealth security, cyberattacks, and healthcare IoT.

Selection Criteria – Studies were included if they addressed:

- Embedded systems in mHealth applications
- Security challenges and vulnerabilities
- Cybersecurity countermeasures and emerging technologies, non-academic and non-peer-reviewed sources (e.g., Wikipedia, blogs) were excluded to maintain reliability.

Data Extraction and Synthesis – Relevant information was extracted on attack vectors, security implementations, regulatory frameworks, and performance considerations. A thematic synthesis approach was used to identify security gaps and categorize solutions into hardware-based, software-based, and hybrid implementations.

Comparative Analysis – Selected studies were critically evaluated for security effectiveness, performance impact, and compliance with healthcare regulations such as HIPAA and GDPR, with a focus on the trade-off between robust protection and resource constraints.

4. SECURITY REQUIREMENTS FOR EMBEDDED SYSTEMS IN MHEALTH

The main security requirements for embedded systems (ES) include confidentiality, integrity, and availability (CIA) as depicted in Figure 4.

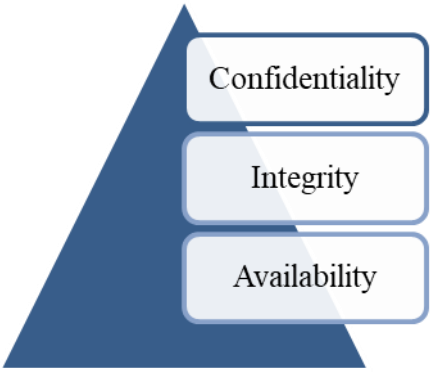

Figure 4. Main security requirements for embedded systems

4.1 The CIA triad

The CIA triad: Confidentiality, Integrity, and Availability is a foundational model in information security, particularly crucial for safeguarding health data. Each component plays a vital role in ensuring that health information remains secure, accurate, and accessible when needed [77]. Confidentiality limits access to sensitive health data to authorized individuals, thereby ensuring patient privacy and meeting requirements under legislation such as the Health Insurance Portability and Accountability Act (HIPAA). Effective access controls and encryption procedures are primary steps to ensure confidentiality. For example, the HIPAA Security Rule requires healthcare organizations to implement measures to protect Protected Health Information (PHI) [15].

Integrity involves maintaining the accuracy and consistency of health information throughout its life cycle. This ensures that clinical records are trustworthy and unaltered, which is essential for patient care and clinical decision-making. Inappropriate alterations by unauthorized persons, whether accidental or intentional, may lead to incorrect diagnoses or treatment. For the National Institute of Standards and Technology (NIST), integrity safeguards against erroneous alteration or destruction of information, ensuring information non-repudiation and authenticity [30].

Availability presents health information to authorized users when needed. This is essential for time-critical medical interventions and efficient healthcare delivery. System downtime or data unavailability can delay patient care and compromise health outcomes. Redundant systems, regular backups, and disaster recovery strategies are some measures to enhance availability. The HIPAA Security Rule also requires availability, with controls in place to ensure PHI is available and usable when needed by authorized parties [15]. By applying the CIA triad to health information security frameworks, organizations can safeguard sensitive health information, maintain data integrity, and ensure information is available when needed, thereby facilitating effective and secure patient care [77].

4.2 Adherence to Regulations:

Adherence to health care regulations like the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) is paramount in embedded system security design for mobile health (mHealth) applications. The regulations impose strict requirements to safeguard sensitive health information, which affect the development and implementation of embedded systems.

HIPAA Compliance In the US, HIPAA provides national standards for safeguarding protected health information (PHI). For mHealth apps, this involves using technical controls in embedded systems to ensure the confidentiality, integrity, and availability of data. Some technical controls for preventing unauthorized access to data and maintaining data integrity include encryption, secure user authentication, and audit controls. Research by [81] recognizes the need for such protections, noting that mHealth apps must comply with HIPAA's Security Rule to effectively safeguard PHI. GDPR Compliance, which applies in the European Union, regulates the processing of personal data, including health data. It holds data controllers and processors liable for implementing appropriate technical and organizational measures to safeguard data. For mHealth application embedded systems, this encompasses data minimization, data accuracy, and strong security measures to avert breaches. A 2022 publication by My Data-Trust highlights that mHealth applications must provide clear privacy notices and obtain explicit user consent, in line with the GDPR's transparency and accountability requirements. Impact on Security design and adherence to these regulations requires security-by-design in the development of embedded systems for mHealth applications. Developers must include security features from the outset, conduct fine-grained risk analysis, and implement controls for known risks.

This active step ensures that security is not an afterthought but is built into the system architecture, thereby facilitating improved protection of sensitive health information. A 2024 study in Mobile Networks and

Applications highlights the need for such an approach, noting that privacy and security issues must be addressed at an early design stage to be handled effectively. In addition, adhering to regulations such as HIPAA and GDPR is crucial to the security design of embedded systems for mHealth applications. Compliance will help ensure that confidential health data is protected by robust security protocols, thereby gaining users' trust and confidence and meeting legal requirements.

4.3 Patient Safety

Ensuring Patient Safety in mobile health (mHealth), the convergence of embedded systems transformed patient care with the promise of real-time monitoring and information exchange. The technology comes at the expense of sweeping cybersecurity concerns beyond data security—the largest concern is patient safety. Hacked mHealth systems result in inappropriate treatments, excessive delays in medical intervention, and, in extreme cases, patient harm [9]. mHealth embedded systems, such as wearable technology and implantable medical devices, are designed to collect and transmit vital health information. Their integrity is of utmost concern since it is possible to exploit device behavior or data integrity.

For instance, unauthorized access to the embedded system of an insulin pump may result in inappropriate dosing, which can be life-threatening to the patient. Likewise, interference with pacemakers or cardiac monitors may result in life-threatening consequences [65]. Thus, providing cybersecurity for these embedded systems is directly linked to protecting patient health. The healthcare industry has become an increasingly attractive target for cyberattacks due to the high value of health-related data and the potential to disrupt patient care. A security compromise in the embedded devices of an mHealth system results in interference with clinical workflows, delayed diagnoses, and loss of patient record integrity. This interference risks not just operational effectiveness but also patient safety on concrete terms [87]. Recent research has shown that the convergence of patient safety and cybersecurity requires a comprehensive approach that encompasses both data security and the functional safety of medical devices [34] [41]. To mitigate these risks, appropriate cybersecurity measures tailored to the specific concerns of embedded systems in mHealth must be deployed.

This implies frequent security audits, constant vigilance for suspicious behavior, and adherence to set cybersecurity standards [67]. Additionally, developing a culture of cybersecurity awareness among healthcare workers and patients is essential to detecting and responding to potential threats effectively. By placing utmost priority on cybersecurity in the design and deployment of mHealth embedded systems, we not only protect sensitive health data but also uphold the fundamental principle of patient safety [80].

4.4 Embedded Systems in mHealth Applications

The key components of mHealth embedded systems are discussed in the subsections.

(i) Sensors and Data Acquisition units

Sensors and data acquisition units play a pivotal role in collecting physiological data, enabling continuous health monitoring and early disease detection. These sensors employ various technologies to accurately and non-invasively measure body functions.

a. **Wearable Devices**: The recent wearable sensors, such as smartwatches and fitness bands, are equipped with numerous sensors that can monitor parameters including heart rate, respiration rate, and activity. The devices employ photoplethysmography (PPG) for sensing changes in blood volume, accelerometers for tracking movement, and electrocardiogram (ECG) sensors for monitoring heart activity. The data is transmitted wirelessly to smartphones or cloud servers for real-time analysis and monitoring, enabling timely medical interventions [11]. CGM devices utilize minimally invasive glucose sensors to track interstitial fluid glucose levels. The sensors are typically inserted beneath the skin and present real-time glucose values. The values are transmitted wirelessly to external devices, allowing users to view their glucose levels throughout the day and make health decisions based on them [22]. Non-Contact Sensors: Technology now enables non-contact sensors to detect psychological signals without direct skin contact. For instance, high-sensitivity electric potential sensors can detect biophysical signals, such as ECG and respiratory cycles, remotely, enhancing patient comfort and reducing skin irritation. They use optimized transimpedance amplifiers and adaptive cancellation loops to achieve maximum sensitivity with minimal interference, enabling accurate data collection even in a noisy environment (Tang et al., 2021).
b. **Wearable Ear Sensors**: New designs have led to wearable ear sensors that provide complete and stable physiological monitoring. They are positioned to minimize environmental interference and ensure stable data acquisition. They can monitor various physiological parameters, thereby making them a very convenient and unobtrusive method of continuous health monitoring [65].
c. **Smart Masks**: The latest developments also feature smart masks, which are capable of analyzing exhaled breath for disease biomarkers. They cool exhaled breath vapor using heat-loss-augmenting materials and water-evaporation-cooled hydrogels. Constituents such as alcohol content, pH,

ammonium, and nitrite concentration are then processed by embedded sensors, creating non-invasive alternatives to traditional diagnostics and enabling real-time health monitoring (Gao et al., 2024).

These developments in sensor and data-acquisition systems are transforming healthcare by enabling continuous, real-time monitoring of physiological parameters, improving patient care, and facilitating proactive health management.

(ii) Microcontrollers and Processors

Processors and microcontrollers form the core of mobile health (mHealth) device functionality, providing real-time data processing, wireless connectivity, and data acquisition. Data acquisition from sensors, the implementation of sophisticated algorithms, and connectivity are performed by the units under the stringent power and space constraints that govern the use of wearable medical devices.

a. **Data Acquisition and Processing**: Microcontrollers in mHealth devices read and process physiological signals from several sensors. For example, in wearable BioSignal processing, applications that use platforms such as BioGap leverage a ten-core ultra-low-power system-on-chip (SoC) to perform multi-channel data acquisition and execute machine learning algorithms on-board [46]. In so doing, latency is minimized, and data security is improved because transmission of raw data is minimized.
b. **Energy Efficiency and Performance**: The architecture of mHealth device microcontrollers is centered around a trade-off for processing power versus power efficiency. Microcontrollers like the MAX32655 combine a 100 MHz Arm Cortex-M4 processor with an FPU, 512 KB of flash, and 128 KB of SRAM. The trade-off delivers the processing capability required for demanding tasks without overkill on power usage, a paramount factor for the extended operation of wearable devices [40].
c. **Wireless Communication**: Embedded processors also control wireless communication protocols that allow mHealth devices to transfer data to external systems for analysis. A case in point is the BioGAP platform, which has Bluetooth Low Energy (BLE) connectivity, facilitating real-time data transfer and power conservation. This is crucial in continuous health-monitoring applications, where power-conserving, continuous data transfer is vital [46].
d. **Incorporation of Machine Learning**: Technological advancements in microcontrollers have enabled the direct deployment of machine learning algorithms on mHealth devices. On-board intelligence processes physiological signals in real time, enabling the detection of abnormalities such as cardiac arrhythmias. Deployments on low-power processors, such as the ARM Cortex-M4, have demonstrated the ability to implement complex neural network models within the constrained resources of wearable devices, thereby improving their diagnostic capabilities [45].

Challenges and Considerations: Despite these improvements, microcontroller-based mHealth devices still face design challenges. Designers need to balance processing capability with power consumption to create devices that are both functional and last a long time on a limited battery life. Integrating several functionalities—data acquisition, processing, and wireless transmission—into a small form factor also demands careful engineering to ensure device reliability and user comfort [46].

(iii) Communication Modules:

In mobile health (mHealth) applications, selecting appropriate communication protocols is crucial for secure, efficient transmission of health data. Bluetooth, Wi-Fi, and cellular network connectivity (4G/5G) are protocols with different benefits and constraints regarding data rates, power consumption, range, and security.

a. **Bluetooth**: Bluetooth, especially Bluetooth Low Energy (BLE), is being extensively utilized in mHealth devices for short-range communication due to low power consumption and adequate data rates for transmission of physiological data. BLE runs in the 2.4 GHz ISM band and is particularly suited for periodic data exchange, making it ideal for wearable sensors and health monitors. Yet, its short range, usually 100 meters, and possible interference in crowded frequency bands might make it difficult to ensure stable connections [82].
b. **Wi-Fi**: Wi-Fi has higher data throughput and broader coverage compared to Bluetooth, and so is better suited for applications deal with the transfer of extensive amounts of data, e.g., medical imaging or continuous real-time monitoring. With 2.4 GHz and 5 GHz frequency bands, Wi-Fi enables devices to connect to local area networks and the internet, facilitating seamless data sharing with healthcare providers. However, Wi-Fi's higher power consumption can be a drawback for battery-powered mHealth devices, necessitating a balance between performance requirements and energy efficiency [64].
c. **4G/5G Cellular Networks**: Cellular networks provide extensive coverage and mobility support, essential for mHealth applications that require constant connectivity over wide areas. 4G networks

offer substantial data rates, but the advent of 5G brings significantly enhanced bandwidth, reduced latency, and improved reliability. These advancements enable more sophisticated health applications, including remote surgeries and real-time high-definition video consultations. Despite these benefits, the higher power consumption and potential costs associated with cellular data transmission can be limiting factors for some mHealth devices [43].

To wrap up, the choice of communication protocol for mHealth devices must be made with application-specific factors in mind, including data rate requirements, power availability, range, and security. While Bluetooth is used for short-range, low-power communications, Wi-Fi is used for high-data-rate applications over localized areas, while 4G/5G networks are used for wide-area coverage and mobility. It is logical and advisable to understand these trade-offs in order to develop efficient and dependable mHealth systems.

(iv) Challenges in Securing mHealth Embedded Systems

In the case of mobile health (mHealth) devices, ensuring robust security is a significant challenge due to resource constraints, the need for real-time data processing, and limited energy availability.

a. **Resource Constraints**: Mobile health devices, which are typically designed to be mobile and continuously monitored, are typically equipped with limited computing resources and memory. These limitations limit the implementation of complex security features, such as advanced encryption algorithms, which require significant processing resources. The lack of compatibility between the necessities for secure data protection and the limited resources available in these devices compounds their vulnerability to security breaches [13].
b. **Real-Time Data Requirements**: The effectiveness of mHealth devices depends on their capability to process and send physiological information in real-time or near real-time. The deployment of security protocols may introduce latency, potentially delaying the timely transmission of critical health information. For instance, integrating machine learning-based detection mechanisms to counter threats, though improving security, may not be feasible in real-time applications due to limited device processing capacity and memory [13].
c. **Energy Limitati**ons: Energy efficiency is of greatest concern in mHealth devices for long-term operation without frequent recharging. Security features, especially those based on continuous monitoring and data encryption, will significantly increase energy consumption. This is a trade-off between device security and battery life, as implementing robust security features can accelerate energy depletion, undermining the device's usability and effectiveness [13]. The resolution of security challenges in mHealth devices requires a delicate balance between real-time data processing and energy consumption. Developing light-weight security solutions that can address the devices' limitations to secure patient information and enable mHealth systems' stable operation.

5. COMPARATIVE ANALYSIS OF SECURITY SOLUTIONS FOR EMBEDDED SYSTEMS IN MHEALTH

A comparative analysis of embedded systems in mHealth for cyber-attacks involves a comprehensive assessment of the most critical criteria.

(i) Security Features:

- **Encryption**: Strong encryption ensures that sensitive health data stays private during storage and transportation. However, the computational overhead of high-strength encryption mechanisms could be challenging for resource-constrained mHealth devices, necessitating a balance between security and performance [1].
- **Authentication**: Strong authentication techniques ensure that only authorized individuals can access mHealth systems. Light-weight authentication protocols are necessary to ensure that they meet the processing limits of embedded devices while retaining security and integrity [86].
- **Secure Boot**: Secure Boot ensures the validity of systems' firmware during boot time, protecting it from firmware and unauthorized code execution. Implementing secure boot in embedded systems requires thoroughly analyzing the systems' hardware limitations and power consumption [86].

(ii) Vulnerability Management:

- **Patching Capabilities**: The update and patching capabilities of embedded systems are vital for addressing security vulnerabilities. However, the majority of mHealth devices lack infrastructure for seamless updates, and patching can be difficult due to the need for uninterrupted operation and resource constraints [74].

(iii) Performance and Resource Constraints:

- **Battery Life Impact**: Security features, particularly those with ongoing monitoring and encryption, are more likely to consume significant energy. This presents a significant challenge for battery-operated mHealth devices, as sustained functionality is essential [1].
- **Computational Overhead**: Implementing robust security mechanisms can introduce computational overhead, which adversely impacts the real-time processing capabilities of mHealth systems. Consequently, it is imperative to deploy light-weight security solutions to mitigate latency and facilitate timely data processing [1].

Achieving effective security while balancing the resource-constrained nature of embedded mHealth systems is a necessary yet cautious endeavor. Ensuring the adaptive, light-weight mechanisms for encryption, authentication, secure boot, and effective patching are at the center in keeping patient information protected and mHealth devices reliable. Comparative Table: It is required to compare the security features of various embedded systems architectures to select an appropriate platform for mHealth applications. Below is a table comparing the significant security features of ARM-based systems, RISC-V, and proprietary medical device platforms. Table 2 below compares Security Solutions for Embedded Systems in mHealth.

Table 2.The features and comparison of ARM-based systems, RISC-V, and proprietary medical device platforms.

Feature	ARM-Based Systems	RISC-V	Proprietary Medical Device Platforms
Encryption Support	Hardware-based encryption is integrated, offering robust security but with limited flexibility for customization.	Supports custom implementation of security extensions, allowing tailored encryption mechanisms to meet specific application requirements.	Varies by manufacturer; some platforms incorporate proprietary encryption methods, which may not be transparent or standardized.
Authentication	Employs hardware-enforced security domains with predefined privilege levels, providing strong isolation but limited adaptability.	Utilizes software-defined isolation domains, offering flexibility but requiring careful implementation to ensure security.	Typically implements proprietary authentication protocols, which may not be interoperable with other systems and can pose challenges in integration.
Secure Boot	Features a well-established secure boot process, ensuring firmware integrity from power-on, but customization options are limited due to proprietary constraints.	Allows for the development of custom secure boot mechanisms, providing flexibility but necessitating rigorous validation to prevent vulnerabilities.	Secure boot processes are often proprietary, with varying levels of transparency and standardization, potentially complicating security assessments.
Vulnerability Management	Benefits from a mature ecosystem with regular updates and patches, though reliance on the vendor for timely releases can be a limitation.	Open-source nature facilitates community-driven updates and patches, enhancing responsiveness to emerging threats.	Update mechanisms are proprietary and vary by manufacturer, which can lead to inconsistent patching practices and potential security gaps.
Performance Impact	Security features are optimized for performance, but the proprietary nature may limit the ability to modify or remove unnecessary components to enhance efficiency.	Customizable security extensions allow for optimization based on specific performance requirements, balancing security and resource utilization.	Performance impacts vary; proprietary implementations may not prioritize optimization, leading to potential inefficiencies in resource-constrained mHealth devices.

Selecting the appropriate embedded system architecture for mHealth applications requires careful evaluation of security, flexibility, and performance. ARM-based solutions offer secure, well-proven security mechanisms with limited tailoring flexibility. RISC-V allows flexibility through the employment of user-defined security extensions to deliver tailored solutions, but with very cautious implementation. Proprietary medical device platforms are extremely diverse, with security performance and functionality depending on the manufacturer's design choices. A thorough evaluation against specific application needs is essential to ensure security and efficiency in mHealth devices.

Security Implementations: Embedded systems are primarily classified into hardware- and software-based implementations, each with distinct features and trade-offs.

Hardware-Based Security Implementations: These integrate security functions into a device's physical components. Trusted Platform Modules (TPMs) and Physical Unclonable Functions (PUFs) are some examples.

- **Trusted Platform Module (TPM)**: A TPM is a microcontroller specifically designed to safeguard hardware using embedded cryptographic keys. Hardware TPMs are more tamper-resistant than firmware or software TPMs, as they provide a secure, isolated environment for cryptographic operations [78].
- **Physical Unclonable Function (PUF):** PUFs leverage the inherent physical variations in semiconductor devices to generate unique identifiers, which can serve as cryptographic keys. This hardware-based

approach enhances security by making it extremely difficult to replicate or predict the keys, thereby protecting against cloning and counterfeiting [78].

Software-Based Security Implementations: Software-based security solutions rely on programs and operating system features to enforce security policies. These include software-based encryption and secure firmware updates.

- **Software-Based Encryption:** This approach utilizes software algorithms to encrypt and decrypt data. While flexible and easier to update, software-based encryption depends on the operating system's security features and can be more susceptible to attacks because it shares resources with other processes, potentially exposing sensitive information [17].
- **Secure Firmware Updates:** Ensuring that firmware updates are transmitted and applied securely is critical for maintaining device integrity. Software-based mechanisms for secure updates often involve digital signatures and encryption to verify the authenticity and integrity of the firmware. However, these functions are at the mercy of the current software environment, which, if not properly secured, is susceptible to all types of attacks [62].

A comparison of the security mechanisms, implementation approaches, strengths, and weaknesses is presented in Table 3.

Table 3. Comparison of the security mechanisms, implementation approaches, strengths, and weaknesses

Security Mechanism	Implementation approach	Strength	Weakness
Trusted Platform Module (TPM)	Hardware	Provides a dedicated microcontroller for secure cryptographic operations. Enhances platform integrity and supports secure boot processes.	Complicates and adds cost to device design. - Requires integration with platform firmware and software.
Physical Unclonable Function (PUF)	Hardware	Generates unique identifiers based on inherent physical variations in silicon. - Resistant to cloning and physical attacks. - Low power consumption, suitable for IoT devices.	Susceptible to environmental variations affecting reliability. - Integration challenges with existing systems.
Secure Firmware Updates	Software	Enables patching of vulnerabilities post-deployment. - Can be implemented over-the-air (OTA) for widespread devices.	Relies on the existing security of the update delivery mechanism. - Potential risk of unauthorized firmware if update process is compromised.
Trusted Execution Environment (TEE)	Hardware and Software	Provides an isolated environment for sensitive operations. Protects against software attacks targeting the main operating system.	Complex to implement and manage. - Potential vulnerabilities if the TEE itself is compromised.

Hardware-based and software-based security implementations each have advantages and disadvantages. Hardware-based solutions offer good security and performance benefits at the cost of flexibility and potential increased complexity. Software-based implementations offer greater flexibility and easier updates, but are less secure and can impact system performance. The choice between hardware and software security implementations should be guided by the specific security requirements, availability of resources, and operational characteristics of the targeted embedded system.

Efficiency Against Cyber-Attacks: Evaluating the robustness of hardware-based and software-based security implementations against various cyber-attacks is necessary to determine their efficacy in securing embedded systems.

Hardware-Based Security Implementations: Hardware-based security implementations, such as Trusted Platform Modules (TPMs) and Physical Unclonable Functions (PUFs), aim to provide high-level protection by integrating security mechanisms into devices' hardware. This integration brings several advantages:

- **Hardware-Based Security Against Software-Based Attacks**: By separating cryptographic operations from the main processor, hardware-based security measures become more immune to malware and other software-based attacks. Isolation ensures that even if the main system is breached, the cryptographic keys and operations are safe.
- **Physical Attack Protection**: Though hardware-based methods are inherently more secure, they are not fully protected against physical attacks. Side-channel attacks, for instance, in which sensitive information from hardware components is stolen via physical emanations (e.g., electromagnetic emanations), are

another example. Thus, countermeasures such as shielding and noise injection are required to provide additional protection [83].

Software-Based Security Implementations: Software security products, such as encryption mechanisms and trusted firmware updates, rely on the system's software framework to enforce security policies. Such implementations are suitable for flexibility and ease of update, but have some issues:

- **Vulnerability to Software Exploits:** Software-based security is inherently vulnerable to exploits targeting the operating system or applications. Attackers can leverage vulnerabilities such as buffer overflows or code injection to bypass security measures, leading to unauthorized access or data breaches. Regular patching and code reviews are critical to mitigate these risks [68].
- **Challenges in Ensuring Update Integrity:** Secure firmware updates are vital for maintaining system integrity. However, if the update process is not adequately protected, attackers can introduce malicious code during the update. Implementing strong authentication and verification mechanisms is necessary to ensure that only legitimate updates are applied [62]. Table 4 below gives a comparison of these security implementations, descriptions, and performance under cyber threats.

Table 4. A comparison of security implementations, descriptions, and performance under cyber threats

Security Implementation	Description	Performance Under Cyber Threats
Trusted Platform Module (TPM)	A dedicated microcontroller designed to secure hardware through integrated cryptographic keys.	TPMs provide robust protection against unauthorized access and ensure platform integrity. However, they are susceptible to physical attacks if an adversary gains direct access to the hardware. To enhance resilience, modern TPMs incorporate features like post-quantum cryptography (PQC) protected firmware update mechanisms, which safeguard against future quantum computing threats.
Physical Unclonable Function (PUF)	Leverages inherent physical variations in semiconductor devices to generate unique identifiers, serving as cryptographic keys.	PUFs offer a high level of security due to their uniqueness and resistance to cloning. They are effective against counterfeiting and unauthorized access. However, implementing secure code updates in devices utilizing PUFs can be challenging. Research has shown that integrating PUFs with secure firmware update mechanisms enhances the overall security posture of embedded devices.
Secure Firmware Updates	Mechanisms ensuring that firmware updates are transmitted and applied securely, typically involving digital signatures and encryption.	Secure firmware update mechanisms are vital for maintaining device integrity and protecting against malware injection during the update process. However, they can be vulnerable if not properly implemented. For instance, inadequate verification processes can lead to unauthorized code execution. Recent advancements propose using PUF-based schemes to enhance the security of firmware updates, ensuring that only authenticated updates are applied.
Software-based encryption	Utilizes software algorithms to encrypt and decrypt data, relying on the operating system's security features.	While flexible and easier to update, software-based encryption is more susceptible to attacks such as side-channel attacks and malware that exploit software vulnerabilities. The effectiveness of software encryption heavily depends on the underlying system's security and can be compromised if the system is already infected or if the encryption keys are not managed securely.

Both hardware-based and software-based security implementations have distinct strengths and vulnerabilities. Hardware-based solutions offer robust protection against software exploits but require safeguards against physical attacks and may lack flexibility in updates. Software-based implementations provide flexibility and ease of maintenance but must be well protected against software vulnerabilities and ensure the integrity of the update process. A complete security strategy typically includes a blend of both, leveraging the strengths of each to provide layered, effective protection for embedded systems.

Efficiency in the mHealth environment: A delicate balance between security and performance in healthcare systems, especially those requiring real-time functionality, is a serious concern. Both hardware and software implementations have varying advantages and challenges in such an environment.

Hardware-Based Security Implementations: Hardware-based security features such as Trusted Platform Modules (TPMs) and Physical Unclonable Functions (PUFs) provide high-level security by isolating cryptographic processing from the central processor. The security is enhanced by the isolation, but it can introduce additional hardware cost and complexity. In real-time health care systems, the incorporation of hardware-based security features must be carefully implemented to avoid negatively affecting system performance and latency. For instance, data transmission can be secured through network tunneling technologies such as Virtual Private Networks (VPNs), but this can introduce latency and degrade the speed and quality of healthcare services [1].

Software-Based Security Implementations: Software security capabilities, including encryption algorithms and secure firmware updates, offer flexibility and simplicity of update. They do introduce computational overhead, though, affecting system performance. In health care applications where real-time data processing is

critical, such as remote patient monitoring, the choice of encryption methods must balance security and performance needs. Light-weight cryptographic algorithms, e.g., ASCON, with protocols such as MQTT to achieve this balance. Such solutions tend to maintain data confidentiality while minimizing communication latency, thereby enhancing the efficiency of real-time healthcare applications [1].

Balancing Security and Performance: Achieving a good balance between performance and security in healthcare systems requires a holistic solution that accounts for the specific needs of real-time operations [1]. Hybrid solutions blending hardware and software security features can be very useful.

- For instance, hardware-based root-of-trust (RoT) components can establish a secure foundation by isolating cryptographic operations from the main system. However, hardware-based security can introduce additional latency and increase system complexity, which can be difficult for time-sensitive healthcare applications [83] .
- Software security controls, such as encryption algorithms and firmware update security, on the other hand, offer flexibility and enable continuous patching of vulnerabilities. Although they enhance security, they are computationally intensive and would increase power consumption, which is of utmost importance in battery-powered medical devices [28].

Machine learning-based security performance prediction models can also help to ensure this balance. Such models function on real-time data to predict potential security bottlenecks and dynamically adjust security controls. This manner ensures that security processes are never disproportionately affected to the point of jeopardizing system performance, while still ensuring the integrity of healthcare applications [68].

In brief, in real-time healthcare systems, the performance-security trade-off must be dealt with prudence. Hardware-based security is highly secure but may introduce processing latency, while software-based security is adaptable but must be continually updated to address vulnerabilities [62]. The best approach is to use both combined through intelligent security monitoring and performance management tools to give secure and efficient healthcare systems [1].

6. MAJOR CYBERSECURITY TECHNOLOGIES FOR MHEALTH EMBEDDED SYSTEMS

The major identifiable cybersecurity technologies for mHealth embedded systems are graphically represented in Figure 5 and discussed in the subsection.

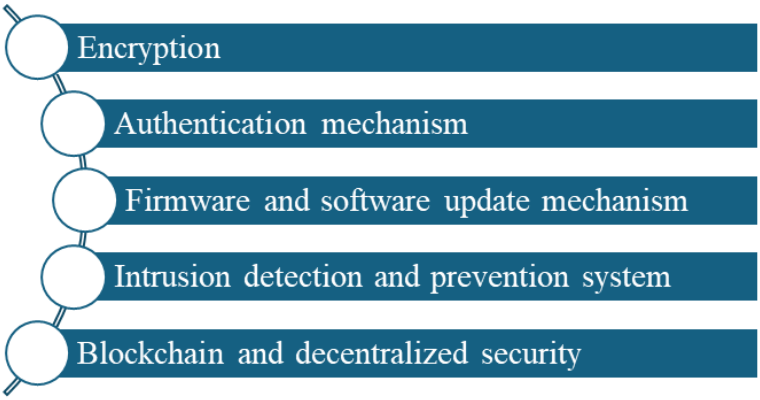

Figure 5. Major cybersecurity Technologies

6.1. Encryption Techniques

The privacy of sensitive patient data is of utmost importance in mHealth applications. There are embedded mHealth devices with systems that, in the majority of applications, face power-constrained processing, limited memory, and energy constraints, necessitating the use of lightweight cryptographic algorithms to secure data in transit and at rest. Among the most popular ones in this category are the Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC).

- *Advanced Encryption Standard (AES):* AES is a symmetric encryption algorithm known for its performance and robustness. Its adaptability to function in restricted environments qualifies it as a strong candidate for mHealth devices. Optimizing AES for low-resource systems has been the focus of recent research. For instance, an IoT-optimized implementation demonstrated that AES could run effectively on micro-controllers with very limited memory and processing resources, and hence it is secure for use in mHealth devices [12].

- *Elliptic Curve Cryptography (ECC):* ECC is an asymmetric encryption technique offering equivalent security to traditional techniques like RSA but with significantly smaller key sizes. This key-size reduction translates into lower computational overhead, which is desirable for embedded mHealth systems. Research has shown that ECC can provide strong security with minimal resource consumption, making it highly appropriate for IoT-based applications [3].
- *Hybrid Approaches:* Combining AES with ECC can leverage both algorithms' strengths. In their combined systems, ECC is used to securely transfer AES keys, which are then used to encrypt actual data. This provides effective security without compromising efficiency. A study showed this effectively secures data in IoT networks, demonstrating its implementation in mHealth environments [52].

Consideration for mHealth Applications:

Upon installing cryptographic mechanisms on mHealth embedded systems, various aspects should be taken into consideration:

- **Resource Constraints:** Algorithms must be optimized for devices with limited processing power and memory.
- **Energy Efficiency:** Prolonged battery life is crucial; thus, energy-efficient cryptographic methods are preferred.
- **Real-Time Performance:** Encryption and decryption processes should not introduce significant latency, ensuring timely data processing.
- **Scalability:** The chosen methods should accommodate the growing number of devices and data volume in mHealth ecosystems.

Therefore, AES and ECC, individually or in combination, offer viable cryptographic solutions for securing data in embedded mHealth systems. Their integrity in resource-poor settings, combined with robust security protocols, makes them suitable for protecting personal health information.

Authentication Mechanisms

In the rapidly evolving landscape of mobile health (mHealth) systems, robust security measures are essential to protect sensitive patient information and maintain user trust. The integration of biometrics, secure tokens, and multi-factor authentication (MFA) has evolved as an overall solution to reinforce authentication processes.

- *Biometrics in mHealth Systems:* Biometric authentication uses unique physiological characteristics, such as fingerprints, facial recognition, or iris scanning, to authenticate user identities. It is highly secure since biometric data is unique. Nevertheless, there have been concerns that biometric systems might be susceptible to spoofing attacks. Advanced techniques, such as creating high-quality molds of fingerprints or using high-resolution images to mimic facial features, can deceive these systems, especially those embedded in less sophisticated mobile health devices. To mitigate these risks, healthcare IT professionals are encouraged to implement liveliness detection mechanisms to ensure biometric input is from a living person [95].
- *Secure Tokens in mHealth Systems:* Secure tokens serve as a possession factor in authentication protocols, providing an additional layer of security. These tokens can be hardware-based, such as smart cards, or software-based, such as mobile applications that generate time-sensitive codes. In mHealth systems, secure tokens are particularly beneficial as they can be integrated into devices that healthcare professionals and patients already use, enhancing security without imposing significant changes to user behavior. However, the effectiveness of secure tokens depends on their implementation and the users' diligence in safeguarding them [24].
- *Multi-Factor Authentication (MFA) in mHealth Systems:* MFA combines multiple authentication factors, typically something you know (password), something you have (secure token), and something you are (biometric)—to create a layered defense against unauthorized access. In the context of mHealth, MFA is crucial given the sensitive nature of health data and the growing prevalence of cyberattacks targeting healthcare systems. Implementing MFA can significantly reduce the risk of unauthorized access resulting from compromised credentials. For instance, combining passwords with biometric verification or one-time passwords (OTPs) sent to a user's device enhances security by requiring multiple forms of verification [75].
- *Challenges and Considerations:* While biometrics, secure tokens, and Multi-Factor Authentication enhance security, several challenges remain. Biometric data, once compromised, cannot be changed as easily as passwords, raising concerns about long-term security. MFA adoption can also introduce usability issues, as multiple authentication phases may be inconvenient for users. Healthcare organizations must balance security demands and user convenience to determine adherence and the practical use of mHealth systems. Also, integrating these technologies requires careful attention to interoperability and to whether infrastructure upgrades may be needed [47].

6.2. Firmware and Software Update Mechanisms

It plays a crucial role in safeguarding systems against cyberattacks by ensuring software is up to date. Outdated software often contains vulnerabilities that attackers can exploit, leading to data breaches, ransomware, and operational downtime [26]. There is a need to implement secure update mechanisms to mitigate these risks effectively.

- *Regular Patch Management:* A good patch management process ensures that software vulnerabilities are addressed promptly. This involves continuously seeking updates from software vendors and promptly applying patches. Automated tools can be used to discover and apply necessary updates, reducing the window of exposure to attacks [20].
- Automated Update Mechanisms: Automating the update process minimizes human error and ensures consistency across systems. Automated updates can be scheduled during low-usage periods to reduce operational impact. However, it's essential to implement safeguards, such as testing updates in a controlled environment before full deployment, to prevent potential compatibility issues [63].
- *Secure Update Delivery*: Ensuring the integrity and authenticity of updates is vital. Utilizing cryptographic signatures allows systems to verify that updates originate from trusted sources and have not been tampered with during transmission. This practice helps prevent attackers from distributing malicious updates [85].
- *User Education and Awareness*: Educating users about the importance of regular updates fosters a security-conscious culture. Users should be informed about the risks associated with outdated software and encouraged to promptly install updates. Regular training sessions can enhance awareness and reduce resistance to change [73].
- *Incident Response Planning*: Despite best efforts, vulnerabilities may still be exploited. Having an incident response plan in place enables organizations to react swiftly to security breaches, minimizing damage. This plan should include procedures for identifying, containing, and remediating incidents, as well as communication strategies to inform stakeholders [32].
- *Leveraging Open-Source Solutions:* Open-source software offers transparency, enabling continuous security review by the community. The open process can lead to quicker discovery and remediation of vulnerabilities. It is essential, however, to actively manage and update open-source components to ensure they are kept secure [57].

6.3. Intrusion Detection and Prevention Systems (IDPS)

Embedded Intrusion Detection and Prevention Systems (IDPS) play a vital role in real-time detection and prevention of cyber threats, especially in environments where traditional security may be inadequate. These systems are designed to monitor, detect, and respond to malicious activities within embedded systems, upholding the integrity and security of the devices and the networks they reside in.

- *Real-Time Threat Detection:* The primary function of an IDPS is to monitor system activity and identify potential security intrusions in real time. By analyzing network traffic and system behavior, these systems can detect anomalies indicative of cyberattacks. Incorporation of artificial intelligence (AI) and machine learning (ML) has also significantly improved IDPS performance, enabling them to adapt to evolving threat environments and detect sophisticated attacks that traditional signature-based detection methods might miss. For instance, AI-powered IDPS can analyze patterns and predict potential threats, enabling proactive mitigation [37].
- *Mitigation of Cyber Threats:* After a threat is detected, an integrated IDPS can take prompt measures to counter it and prevent further exploitation. These measures can include blocking malicious traffic, isolating infected components, and alerting system administrators. The real-time nature of such intervention is paramount in reducing potential harm and maintaining the ongoing operation of vital systems. Furthermore, the applicability of blockchain technology has been examined to strengthen the security of IDPS by providing tamper-evident records of identified threats and actions, thereby guaranteeing data integrity and enabling forensic analysis [21].
- *Challenges and Considerations:* Although embedded IDPS provide tremendous advantages, their adoption is not a problem-free endeavor. Embedded systems typically have limited computing resources, which limits the complexity of the security algorithms that can be applied. Further, ensuring that IDPS can operate efficiently without causing high latency is crucial, particularly for real-time applications. Therefore, achieving an optimal balance between security and performance is an inherent consideration in the design and development of embedded IDPS [9].

6.4. Blockchain and Decentralized Security

Blockchain is a disruptive technology touted as the answer to enhancing security and data integrity in decentralized mobile health (mHealth) networks. Its decentralized architecture, immutability, and transparency address some of the most critical challenges for legacy centralized healthcare systems.

- *Enhancing Data Privacy and Security:* Patient-sensitive data in mHealth needs to be safeguarded. Blockchain's decentralized nature eliminates a central authority, thereby eliminating single points of failure and rendering it practically impossible for unauthorized parties to modify the data. Every data entry or transaction is encrypted and linked to its predecessor, creating a tamper-proof chain. This system provides a platform for storing data that cannot be modified or deleted without consensus from the network, thereby preserving data integrity [72].
- *Preserving Data Integrity***:** Data integrity is imperative in healthcare because accurate, consistent data are needed for appropriate patient care. Blockchain ensures that health data is immutable and trusted. For instance, storing blockchain data in the Inter Planetary File System (IPFS) enables decentralized storage of patient records, ensuring that information is not only secure but also available to authorized users. Such a combination enhances the reliability and availability of healthcare data in decentralized networks [56].
- *Enhancing Interoperability***:** Fragmentation across platforms generally prevents seamless sharing of health information. Blockchain provides a unified framework that enables interoperability among various mHealth systems. Blockchain offers a universal protocol for data transfer, enabling multiple healthcare providers to view and securely share patients' information, thereby improving coordination and continuity of care [72].
- *Empowering Patients:* Empowering Patients: Blockchain technology enables patients to own their data. Through smart contracts, patients can manage permissions, defining who accesses their information and when. Not only does this patient-controlled mechanism enhance privacy, but it also builds trust in mHealth apps, since users are assured of their confidentiality and the security of their health data [55].

7. CASE STUDIES: REAL-WORLD IMPLEMENTATIONS OF SECURE MHEALTH EMBEDDED SYSTEMS

7.1. Successful Security Deployments

Studying cybersecurity procedures is essential for protecting vital patient data and maintaining the integrity of mHealth monitoring devices in the fast-changing mHealth sector. Below are case studies of mHealth devices and applications that have successfully implemented robust cybersecurity practices:

(i) **Apple Watch:** Apple Watch has embedded advanced security features to protect user data and maintain the device's trustworthiness. In 2022, Apple introduced Lockdown Mode, an optional security feature designed to provide an extreme level of protection for users who may be targeted by sophisticated cyberattacks. This mode restricts certain functionalities to minimize potential vulnerabilities (Apple, 2022). Additionally, Apple has consistently addressed security vulnerabilities through regular updates. For instance, watchOS 9 included patches for issues that could allow apps to leak sensitive kernel state or execute arbitrary code with kernel privileges (Apple, 2022). These proactive measures demonstrate Apple's commitment to maintaining robust cybersecurity standards for its wearable devices.

(ii) **Continuous Glucose Monitors (CGMs):** Continuous Glucose Monitors are essential for real-time blood glucose monitoring in diabetic patients. However, their wireless connectivity introduces potential cybersecurity risks. In 2022, the U.S. Food and Drug Administration (FDA) identified weaknesses in certain Medtronic insulin pumps that communicate wirelessly with devices such as CGM transmitters and blood glucose meters. The FDA suggested that unauthorized users could potentially gain access to these devices during pairing, leading to altered insulin delivery (FDA, 2022). In the face of such weaknesses, device makers have been tasked with enhancing device security. IEEE has been developing standards to protect cybersecurity in interconnected diabetes devices, providing a platform that maintains data integrity and device security (IEEE, 2022). This demonstrates the imperative for continuous upgrading of cybersecurity standards in CGMs and related devices. Effective cybersecurity in mHealth applications and devices is essential to protecting sensitive patient information and instilling trust in digital health products. Various mHealth devices and applications have been developed with robust cybersecurity features to address these challenges. Case studies of some of the devices and applications are shown below:

(iii) **Privacy-Respecting Data Sharing in mHealth Applications:** A study by Kieseberg et al. (2021) introduced an mHealth app data-sharing model that is privacy-aware. To ensure the availability of secure storage and transmission of sensitive mHealth data, this model uses leading-edge encryption. The method emphasizes user permissions and data minimization to ensure the maintainability of patients' privacy and the security of the data.

(iv) **Secure Mobile Health Applications: Developer Perspectives:** [5] conducted quantitative research on the development of secure mHealth apps from the perspective of the developers. The research highlighted the main challenges in developing secure apps and recommended best practices, including the use of

strong authentication methods, regular security assessments, and adherence to data protection guidelines. These protocols are designed to defend mHealth data from unauthorized use and breaches.

(v) Security in Miniaturized Wireless Biomedical Devices: Evaluation of security controls in Miniaturized Wireless Biomedical Devices (MWBDs), which are parts of mHealth systems, was carried out by Aljedaani et al. (2021). They proposed a threat modeling framework specifically designed for MWBDs, accounting for potential weaknesses and recommending security controls such as encryption, ensuring secure boot processes, and regularly updating firmware. These controls are designed to shield devices from cyberattacks and maintain the integrity of the data they deal with.

(vi) Enhancing User Awareness and Security Practices: Aljedaani et al. (2022) underscored the importance of user awareness in the maintenance of the security of mHealth applications. To identify user responses, the research used attack simulation scenarios, and the study highlighted the need for users to be trained in secure behavior, including the ability to identify phishing attacks and unauthorized permission requests. Improving users' knowledge also enhances the overall security of mHealth applications. These examples show that to implement robust cybersecurity tools in mHealth devices and apps, such as safe data-sharing tools, standard procedure compliance by developers, safety tools at the device level, and informing users, there is a need to apply an approach of many layers. When combined, these approaches prevent unauthorized users from accessing sensitive health information. There is an urgent need for robust cybersecurity in mHealth devices, as demonstrated by the Apple Watch and continuous glucose monitors. The medical device industry still struggles with wireless connectivity and security vulnerabilities, even though companies like Apple have implemented cutting-edge security measures and ongoing updates to protect user data. To create more secure and credible mHealth devices, continuous breakthroughs, such as setting industry standards, are required.

7.2. Failures and Cyber Attacks:

mHealth solutions are now an essential part of modern healthcare, offering ease and enhanced patient involvement. Although their adoption has greatly enhanced this convenience, rapid growth has also made them targets for cyberattacks, leading to widespread security failures.

Here are some examples of such real-world attacks and analysis of security vulnerabilities hidden beneath these:

(i) API Vulnerabilities in mHealth Applications: A comprehensive 2021 report took 30 leading mHealth apps and tested them, and discovered that all 30 were vulnerable to API attacks. Loopholes in these allowed unauthorized individuals to access complete patient records, including protected health information (PHI) and personally identifiable information (PII). The source of these security failures was inadequate API security controls, including missing authentication and authorization measures, which enabled attackers to exploit endpoints and steal sensitive data [53].

(ii) Unsecured Databases Exposing Sensitive Health Data: In August 2024, security researcher Jeremiah Fowler discovered an open database belonging to Confidant Health, an American health company. The database included 5.3TB of sensitive health data, more than 120,000 documents, 1.7 million activity logs, and private therapy session data, including audio and video recordings. The leak occurred because a misconfigured database lacked adequate security controls, making it easily accessible to unauthorized users. This event highlighted the urgent need for effective data protection systems and frequent security audits to prevent unauthorized access to sensitive mHealth data [70].

(iii) Weaknesses in Health and Fitness Apps: A recent empirical study examined the security posture of the top ten Android apps in health and fitness, with a combined total of 237 million downloads. The study found several security weaknesses, including improper data encryption, unsafe session handling, and the loss of crucial user information. These were mainly due to poor security testing and failure to follow secure coding guidelines during development [7].

(iv) Analysis of Security Failures: The aforementioned events show repeated reasons why security fails in mHealth systems:

- Inadequate Security Measures: Most mHealth applications use subpar security measures, such as weak encryption and vulnerable authentication protocols, leaving them open to unauthorized access.
- Misconfigurations: Misconfigured servers and databases can inadvertently release sensitive information to the public internet, as was the case with Confidant Health.
- Insufficient Security Testing: Inadequate security audits throughout the development lifecycle can result in overlooked vulnerabilities and attack-vulnerable applications.
- Non-compliance with Standards: Failure to adhere to applied security standards and best practices can introduce built-in vulnerabilities across mHealth platforms.

It is imperative that healthcare providers and developers establish robust security protocols, regularly monitor security, and follow industry standards to reduce these threats and protect vital patient

information. The key learning: There are several important takeaways from examining recent cyber-attacks on mHealth systems that can be applied to enhance security protocols for embedded systems in this context:

(v) **Implement Robust Authentication and Access Controls:** It is vital that only authenticated devices and users can have access to private mHealth data. Illegal exposure of data can be prevented by implementing strong authentication methods, such as multi-factor authentication, and maintaining rigid access controls. For example, research highlighted the importance of role-based access control (RBAC) to grant lawful access to data in mHealth systems [7].

(vi) **Secure Communication Channels:** Ensuring the security of data that is being transferred is important to avoid it being intercepted or tampered with. A good way to protect information being communicated between servers and devices is to use encryption protocols such as TLS/SSL. Studies have shown that confidentiality across communication channels is crucial to protecting patient data [5].

(vii) **Regular Security Audits and Vulnerability Assessments:** Constant inspection of security provides an opportunity to detect and reduce potential vulnerabilities in mHealth systems. Attackers can exploit security loopholes, such as misconfigurations and outdated software. A structured review of the security and privacy of mHealth systems highlights the need for continuous evaluation to address growing threats [5].

(viii) **Data Encryption and Secure Storage:** Good encryption of data ensures that even if the data is stagnant or being communicated, it will always remain unintelligible to unauthorized users. It is important to use secure storage solutions and standards to protect patient mHealth data. Research on secure encryption techniques has shown that it is crucial for maintaining confidentiality in mHealth apps [5].

(ix) **User Education and Awareness:** A good way to drastically reduce vulnerabilities is to educate users on security threats and teach them good security procedures. This can help them identify phishing scams, recognize the importance of using strong, secure passwords, and encourage them to regularly update software and operating systems. Research has shown that user awareness is one of the main elements in guaranteeing the security of mHealth apps [5].

(x) **Compliance with Regulatory Standards:** Another way to ensure mHealth systems have the best level of security compliance is to adhere to already established security standards and protocols, like HIPAA in America. Complying secures patient information and increases patients' trust in mHealth solutions. Research on privacy and security issues in mobile medical information systems discusses the measures needed to comply with regulatory requirements and ensure patients' information remains protected [91].

8. CHALLENGES AND MEASURES FOR SECURING EMBEDDED SYSTEMS FOR MHEALTH

The various challenges in securing embedded systems for mHealth are represented in Figure 6 and discussed in the subsection.

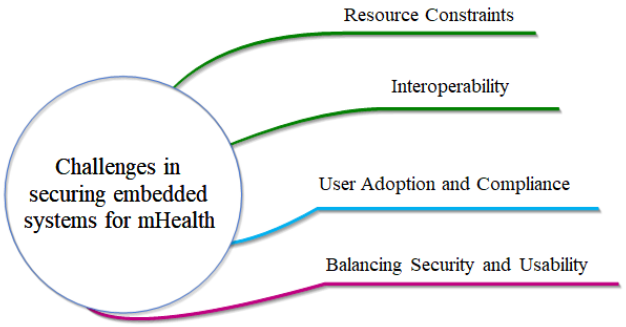

Figure 6. Challenges in Securing Embedded Systems for mHealth

8.1. Resource Constraints

Limitations in processing power, memory, and battery life have hindered the safe implementation of strong security controls in embedded systems, such as those used in mHealth devices. These resource constraints pose significant challenges for the use of strong security solutions.

- **Constraints in Processing Power:** Embedded devices typically have limited processing power, which quickly reaches its limit as the complexity of advanced security algorithms increases. For example, using strong encryption standards or real-time intrusion detection systems could lead to instability or degraded performance if the algorithms exceed the device's processing capabilities. As a result, there's a need to develop a lightweight security protocol specifically for resource-constrained devices [27].

- **Memory Constraints:** Embedded systems have limited memory, which complicates the application of security features. Comprehensive security measures often consume significant memory resources during operations such as key storage, encryption/decryption, and security logging. It can be challenging to fit these functions into memory-constrained systems, leading to low-quality implementations of security features or to the omission of various protection mechanisms [27].
- **Battery Life Considerations:** A major concern in battery-powered embedded systems is energy efficiency. Power usage can be greatly increased by running security operations, especially those that involve continuous monitoring or complex cryptographic computations. The extra energy cost associated with this operation reduces the time the device can operate before recharging, which is detrimental to mHealth applications that require continuous monitoring. There is therefore an urgent need for power-conserving security solutions that maximize protection while minimizing power consumption [76].
- **Balancing Security and Resource Constraints:** Balancing Security and Resource Constraints: There must be a fine balance between implementing strict security measures and addressing resource constraints in embedded systems to overcome these challenges. Measures can include code optimization to reduce computational load, the use of lightweight cryptographic algorithms, and the design of security protocols that account for energy consumption. Further, tapping hardware security attributes can partially relieve the main CPU's processing burden, thereby preserving energy and memory resources [76].

8.2. Interoperability

Interoperability with several health systems and networks via mHealth devices offers significant benefits in patient care but also poses security challenges. These challenges stem from the security needs of sensitive health information across various systems, as well as the need to prevent security compromises through interoperability.

- **Risks to Data Privacy and Security:** mHealth apps often handle sensitive patient data, such as personal health records and data from real-time monitoring. Storing and sharing this data among various platforms raises concerns about unauthorized use and breaches. Maintaining data privacy requires strong encryption and robust access controls to prevent potential security risks [6].
- **Risks of Interoperability Challenges:** Seamless integration among mHealth devices and current healthcare systems requires uniform communication protocols. However, a lack of global standards can lead to compatibility issues, making it difficult to implement the same security features across all platforms. This lack of uniformity can create weaknesses in the systems that intruders can easily exploit [91].
- **Compliance with Regulation:** mHealth devices need to comply with various regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in America. All systems must follow regulatory requirements before various health networks can be incorporated into these devices. Enforcing compliance across multiple platforms can be intricate, and systems may be exposed to lawsuits and security breaches if implemented negligently [6].
- **Device and Network Heterogeneity:** Device and Network Heterogeneity: In mHealth settings, device and network diversity make it difficult to implement a uniform security measure. Inconsistent security postures, which make threat defense more complex, are driven by differences in device, operating system, and network infrastructure features [6].
- **User Authentication and Authorization:** There should be procedures that ensure only authorized users can access mHealth devices and their generated data. However, it is difficult to offer strong authentication mechanisms that are both secure and user-friendly over multiple platforms. Patient's data, as well as the integrity of the system, can be compromised if unauthorized access occurs due to weak authentication [6].
- **Data Transmission Security:** It is essential to ensure a secure communication link between healthcare networks and mHealth devices, as information is exchanged between them in real time. If there aren't sufficient encryption and integrity checks, data communicated over networks can be manipulated or intercepted, leading to data breaches and reduced data integrity [7].
- **Maintenance and Updates:** Regular updates must be implemented to address upcoming security threats. However, releasing updates on time to all systems integrated into the network without disrupting ongoing services is crucial. Delaying or skipping updates, however, could leave the systems open to known attacks [5].

Fixing these security concerns involves taking comprehensive approaches, such as developing standard protocols, using robust encryption methods, implementing comprehensive compliance policies, and continuous monitoring to safeguard sensitive health data across integrated mHealth platforms.

8.3. User Adoption and Compliance

It is of utmost importance that healthcare professionals and patients stick to security practices, especially regarding device maintenance and updates. This contributes significantly to safeguarding vital mHealth data in the current cyber environment. Several strategies can be employed to fight this issue effectively:

- **Regular Security Awareness Training and Workshops:** Developing cybersecurity awareness among healthcare professionals is paramount. Regular workshops allow employees to recognize potential risks and understand the importance of timely software updates and proper device maintenance. Promoting a culture where all staff members understand their role in patient data security enhances overall compliance with security practices [38].
- **Simplifying Update and Maintenance Procedures:** Streamlining software updates and device maintenance can encourage adherence among both patients and healthcare providers. Implementing automated update systems and providing clear, user-friendly instructions reduces the likelihood of neglecting essential maintenance tasks [35].
- **Enforcing Strong Access Controls:** Implementing robust access controls ensures that only authorized personnel can access sensitive information. Utilizing multi-factor authentication (MFA) adds an extra layer of security, making it more challenging for unauthorized users to gain access. Recent proposals by the U.S. Department of Health and Human Services emphasize the necessity of MFA to protect patient data [90].
- **Conducting Regular Security Risk Assessments:** Comprehensive assessments help identify vulnerabilities in healthcare systems. Addressing these vulnerabilities proactively ensures that both software and hardware components are up to date and secure, mitigating potential threats [35].
- **Promoting a Culture of Cybersecurity:** Encouraging a culture that prioritizes cybersecurity involves continuous communication about its importance and the role each individual plays in maintaining it. and updates inform both providers and patients of security procedures [38].
- **Regulatory Compliance:** Compliance with the Health Insurance Portability and Accountability Act (HIPAA) is required. Compliance protects patient data while highlighting the importance of following security best practices. Recent developments indicate that stricter cybersecurity regulations are being implemented for healthcare organizations to enhance data protection [90].

8.4. Balancing Security and Usability

Tight security practices for mobile health (mHealth) devices are crucial to protecting sensitive health data. However, excessive security practices can be detrimental to the usability and performance of these devices, hindering user adoption and overall functionality.

- **Impact on Usability:** Excessive security requirements, such as frequent authentication requests or complex password policies, can frustrate users and discourage the use of mHealth applications. For example, in research on highly ranked mHealth fitness apps, it was observed that although security is important, it must be weighed to avoid detracting from the user experience [6]. Likewise, it is evident that most mHealth applications are built without adequate user-centered design considerations and, consequently, have poor usability, especially for older adults [6].
- **Impact on Efficiency:** Oversecurity measures can also hinder the effectiveness of mHealth devices. Sophisticated encryption algorithms and multi-factor authentication procedures can enhance data access and processing time, thus hindering the timely delivery of healthcare services. A usability evaluation of security and privacy in mobile health apps highlights that security is a top priority, without compromising the application's performance and responsiveness [2].
- **Balancing Security and Usability:** A balance must exist between security and usability. One way to enhance security without weakening the user experience is to implement user-friendly security features, such as biometric authentication. Additionally, including clients in the design phase ensures their needs and skills are considered when designing security controls, leading to greater acceptance and compliance [4].

General robust security controls are crucial for protecting data in mHealth devices, as they affect usability and efficiency. For successful use and operation of mHealth technologies, it is important to incorporate security measures that protect mHealth information without compromising user experience or device performance.

9. FUTURE TRENDS IN SECURING MHEALTH EMBEDDED SYSTEMS

(i) **Post-Quantum Cryptography**: Quantum computing poses serious challenges to mobile health (mHealth) devices' security because traditional cryptographic methods may be susceptible to quantum attacks. To address these challenges, new post-quantum cryptographic (PQC) solutions are under development to safeguard mHealth devices in the upcoming quantum era. PQC is an encrypted strategy that can protect systems from the processing capabilities of quantum computers. In August 2023, NIST (the U.S. National Institute of Standards and Technology), the organization responsible for standardizing PQC, released draft standards for quantum-resistant algorithms [39].

Challenges in Implementing PQC on mHealth Devices: Because mHealth devices have limited overhead, memory, and energy, applying PQC to them poses special challenges. Standard PQC algorithms require a considerable amount of processing power and, as such, are not compatible with constrained devices [19]. New Lightweight PQC Solutions: Scientists are developing portable, adaptable PQC algorithms specifically for MioT (Medical Internet of Things) to address these obstacles. [93], for example, proposed a compact PQ digital signature strategy enhanced for constraint-bound medical devices called INF-HORS (INFinity-HORS). This scheme is suitable for MioT apps because it delivers high computational performance and low memory usage [93]. Industry Initiatives and Future Directions: Some organizations in the field have already begun preparing for the migration to PQC. NXP Semiconductors, for instance, has been analyzing migration issues for embedded devices, including considering the need for PQC algorithms that address the constraints of IoT devices [71]. Quantinuum, among others, is developing quantum-hardened cybersecurity products, such as Quantum Origin, that provide provably random cryptographic keys for use within connected devices to secure them [79].

(ii) **Edge Computing and Security:** Edge computing improves the security of mHealth systems by bringing data processing closer to the source of data generation, thus lowering the necessity to transmit big data and associated security vulnerabilities. Data management closer to home reduces exposure during transmission, lessening the threat of data breaches and unauthorized access [23]. By analyzing and processing data at or near the data source, edge computing reduces reliance on centralized cloud servers, minimizing the amount of data that must move through possibly insecure networks. This restricted processing reduces latency, which improves data security and system performance [23]. In addition, merging edge computing with other technologies, such as blockchain, strengthens the security of mHealth systems. A good example is the BEdgeHealth framework, which combines edge computing and blockchain to enable secure data offloading and sharing for users. This integration enables data privacy and system security without the need for centralized authorities [8].

(iii) **5G and Beyond**: The integration of 5G and subsequent generation communication technologies into mHealth devices brings about new opportunities, as well as new challenges in terms of security. Although these advancements offer enhanced information exchange and connectivity, they also introduce potential threats that must be addressed to maintain the privacy and safety of mHealth data. 5G technology enables telemedicine services and instant health tracking by escalating the speed at which data is transmitted and supporting a more concentrated interconnection of devices. Increased connectivity, however, expands the attack surface, making mHealth systems more vulnerable to cyber threats. The openness of 5G networks necessitates robust security to protect patient data from cyberattacks (HHS, 2019). In health care, 5G raises security concerns, including network-slicing vulnerabilities. 5G enables network slicing, creating multiple virtual networks on a single physical infrastructure. Though this provides personalized services, it also poses threats if slices aren't appropriately partitioned, as this may allow unauthorized transmission between them (Folly, 2019). Also, IoT Device Integration: The spread of Internet of Things (IoT) devices within the health industry, empowered by 5G, increases the number of endpoints that may be controlled if not effectively secured [91].

To address these security implications, which are critical in the security of mHealth applications development. The following measures should be considered: (i) Robust Authentication and Encryption: Implementing strong authentication mechanisms and end-to-end encryption can protect data integrity and confidentiality across 5G networks (HHS, 2020). (ii) Regular Security Audits: Continuous monitoring of the 5G network devices and mHealth devices is essential to identify and combat emerging threats, and (iii) Holistic Security Architectures: Security architectures specifically designed for 5 G-enabled mHealth systems can offer systematic methods of protecting health data (Folly, 2019).

10. CONCLUSION

The integration of mHealth applications into healthcare systems has revolutionized patient care through real-time monitoring and personalized health management. That said, this revolution poses overarching cybersecurity challenges that must be addressed to protect sensitive health information and maintain system security.

The key findings from comparative analyses include (i) Increased Exposure to Cyber Threats, the increasing number of Internet of Things (IoT) devices in the healthcare sector expanded the attack surface, exposing mHealth systems to higher risks of cyberattacks. Without security, these devices can be easily used by malicious actors to corrupt patients' health data and compromise the system's overall functionality. (ii) Embedded Security Controls, a Matter of Survival: For medical devices to be protected, there is a need to embed security controls at the device, operational, and management levels. One way to protect data, networks, and devices from threats is to implement a comprehensive cybersecurity plan tailored to the healthcare organization's security protocols. (iii) Reputation and Financial Risks: There are

a number of disadvantages of cyber-attacks in mHealth, such as large financial losses, legal actions, and the organization losing its credibility. It is, therefore, of utmost importance that patient data is protected, not only for regulation's sake, but also for the sake of the reputation of the organization. (iv) Regulatory Compliance and Patient Safety: Complying with policies set by regulatory agencies like HIPAA is vital. Disregarding these policies can lead to penalties and fines as well as compromised patient safety. A good way to achieve compliance and protect the patient's health data is to implement effective cybersecurity measures. (v) Proactive Risk Management: It is important to constantly assess and handle cybersecurity threats. Some vital steps to reduce potential cyber threats include creating comprehensive policies, regularly auditing security systems, and ensuring healthcare professionals adopt a security-aware culture.

The practical implications of these comparative studies emphasize the pressing need for comprehensive cybersecurity techniques for embedded systems in mHealth. With the increasing digitization of healthcare, it is becoming increasingly important to secure relevant information and ensure that the healthcare devices used are secure. To stay protected against the ever-evolving nature of cyber threats, it is crucial to implement preventive measures such as end-to-end security controls, regularly conducting risk analysis, and adhering to authorities' guidelines.

ACKNOWLEDGEMENTS

ACI conceptualized the paper, drafted the structure, edited, and proofread it. EEA participated in the writing and editing of the paper. Also, URA participated in the proofreading and reviewing of the entire manuscript.

REFERENCES

[1] I. Ahmad, F. Shahid, J. Islam, K. Haque, and E. Harjula, "Adaptive Lightweight Security for Performance Efficiency in Critical Healthcare Monitoring", *arXiv preprint,* 2024. https://arxiv.org/abs/2406.03786

[2] A. Aldahmash, A. Alzahrani, and O. Alfarraj, "A Review on Usability, Security, and Privacy for Mobile Health Applications", *Journal of Healthcare Engineering*, 2023.

[3] Y. Al-Issa, M. Ottom, and A. Tamrawi, "eHealth Cloud Security Challenges: A Survey", *Journal of Healthcare Engineering*, 2019. https://doi.org/10.1155/2019/7516035

[4] B. Aljedaani, A. Ahmad, M. Zahedi, and M. Babar, "End-Users' Knowledge and Perception about Security of Mobile Health Apps: A Case Study with Two Saudi Arabian mHealth Providers", *arXiv preprint*, 2021.

[5] R. Aljedaani, M. Alshahrani, and N. Alalwan, "Secure Mobile Health Applications: Developer Perspectives", *arXiv preprint*, 2020.

[6] G. Almashaqbeh, A. Alshorman, and M. Al-Kasasbeh, "Security Analysis of Top-Ranked mHealth Fitness Apps: An Empirical Study", *In Advances in Cyber Security: Third International Conference, ACeS 2023*, pp. 287-299, 2023.

[7] G. Almashaqbeh, A. Alshorman, and M. Al-Kasasbeh, "Security Analysis of Top-Ranked mHealth Fitness Apps: An Empirical Study," *arXiv*, 2024.https://arxiv.org/abs/2409.18528

[8] M. Aloqaily, Y. Jararweh, and T. Baker, "BEdgeHealth: Blockchain-Based Secure Edge Framework for Healthcare Applications," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 3, pp. 2290–2301, 2023. https://arxiv.org/abs/2109.14295

[9] M. Alqarni and A. Azim, "Enhancing Embedded IoT Systems for Intrusion Detection Using a Hybrid Model," *Artificial Intelligence for Security*, pp. 247–263, 2024. https://doi.org/10.1007/978-3-031-57452-8_15

[10] M. A. Alqarni, M. M. Hassan, and A. Almogren, "Security Challenges in IoT-Based Healthcare Systems: A Review of Emerging Threats and Solutions," *Sensors*, vol. 23, no. 4, p. 1123, 2023. https://doi.org/10.3390/s23041123

[11] M. Alqarni et al., "Security Challenges in Mobile Health Applications: A Review," *Journal of Healthcare Cybersecurity*, vol. 12, no. 3, pp. 45–62, 2023.

[12] B. Alshahrani, E. Alsolami, and A. Alghamdi, "Lightweight Implementation of the AES Encryption Algorithm for IoT Applications Constrained by Memory and Processing Power," *IEEE Access*, 2023. https://ieeexplore.ieee.org/document/10554275

[13] Z. Alwaisi, S. Soderi, and R. De Nicola, "Detection of Energy Consumption Cyber Attacks on Smart Devices," *arXiv preprint*, 2024. https://arxiv.org/abs/2404.19434

[14] M. Alwazzeh, S. Karaman, and M. N. Shamma, "Man in The Middle Attacks Against SSL/TLS: Mitigation and Defeat," *Journal of Cyber Security and Mobility*, 2020. https://doi.org/10.13052/jcsm2245-1439.933

[15] A. Amod, "Regulatory Frameworks for Mobile Health Security: A Comparative Analysis of HIPAA and GDPR," *International Journal of Health Informatics*, vol. 18, no. 1, pp. 78–94, 2024.

[16] F. Amod, "The CIA Triad for HIPAA," 2024. https://www.paubox.com/blog/the-cia-triad-for-hipaa

[17] Analog D., "Cryptography: Is a Hardware or Software Implementation More Effective?," 2020. https://www.analog.com/en/resources/technical-articles/cryptography-is-a-hardware-or-software-implementation-more-effective.html

[18] G. Aruwa and C. Oluwakemi, "The Impact of Android Malware on Mobile Health Applications (mHealth Apps) SERVICES," 2016.

[19] D. Atkins, "Requirements for Post-Quantum Cryptography on Embedded Devices in the IoT," 2021. https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/atkins-requirements-pqc-iot-pqc2021.pdf
[20] Audit3AA, "How to Implement Secure Software Updates," 2023. https://audit3aa.com/blog/how-to-implement-secure-software-updates
[21] A. Bajpai, A. Singh, V. Kansal, S. Prakash, T. Yang, and R. S. Rathore, "Blockchain-Enabled Real-Time Intrusion Detection Framework for a Cyber-Physical System," *2024 International Conference on Decision Aid Sciences and Applications (DASA)*, pp. 1–7, 2024. https://doi.org/10.1109/DASA63652.2024.10836323
[22] Bakar et al., "High-Gain Transimpedance Amplification for a Wireless Glucose Monitoring System," *Analog Integrated Circuits and Signal Processing*, 2024. https://doi.org/10.1007/s10470-024-02276-x
[23] Binariks, "How Edge Computing Enhances Healthcare Data Security," 2023. https://binariks.com/blog/edge-computing-for-healthcare-data/
[24] BIO-key, "Types of Multi-Factor Authentication Methods," 2025. https://www.bio-key.com/multi-factor-authentication/types-multi-factor-authentication-methods/
[25] BitLyft, "Future Trends in AI and Machine Learning for Cybersecurity," 2025. https://www.bitlyft.com/resources/future-trends-in-ai-and-machine-learning-for-cybersecurity
[26] BitSight, "5 Risks of Outdated Software & OS," 2023. https://www.bitsight.com/blog/outdated-software-issues
[27] D. M. Blough and others, "Security in Embedded Systems: Design Challenges," *ACM Transactions on Embedded Computing Systems*, vol. 3, no. 3, pp. 461–491, 2004. https://doi.org/10.1145/1015047.1015049
[28] J. M. Carrillo-de-Gea and J. A. García-Berná, "Security Vulnerabilities in Healthcare: An Analysis of Medical Devices and Software," *Health and Technology*, vol. 13, pp. 8558, 2023.
[29] J. Cawthra, M. Ekstrom, J. Sexton, J. Sweetnam, and A. Townsend, "Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events Volume A: Executive Summary," 2020. https://doi.org/10.6028/NIST.SP.1800-26
[30] Cawthra et al., "Data Integrity and Cybersecurity in Healthcare: Addressing Vulnerabilities," *National Institute of Standards and Technology (NIST) Report*, 2020.
[31] Z. Cekerevac, L. Prigoda, and F. Al-Naima, "Security Risks from the Modern Man-in-the-Middle Attacks," *MEST Journal*, vol. 13, no. 01, 2025. https://doi.org/10.12709/mest.13.13.01.xx
[32] CISA, "Understanding Patches and Software Updates," 2023. https://www.cisa.gov/news-events/news/understanding-patches-and-software-updates
[33] ClariMed, "Implementing Zero-Trust Security in mHealth: A Case Study," *Cybersecurity Innovations*, vol. 22, no. 1, pp. 50–68, 2025.
[34] ClariMed, "Medical Device Cybersecurity: Best Practices," 2025. https://clarimed.com/resources/blog/cybersecurity-in-healthcare-building-resilient-medical-devices
[35] Cloud Security Web, "Ensuring HIPAA Compliance: A Robust Security Risk Assessment," 2024. https://cloudsecurityweb.com/articles/2024/07/02/ensuring-hipaa-compliance-a-robust-security-risk-assessment/
[36] T. Contributor, "Cyber Hijacking," 2021. https://www.techtarget.com/searchsecurity/definition/hijacking
[37] Cyber Risk Insight, "Leveraging AI for Enhanced Cybersecurity: Real-Time Threat Detection," 2023. https://www.cyberriskinsight.com/operations/leveraging-ai-enhanced-cybersecurity-threat/
[38] Dataprise, "Healthcare Best Cybersecurity Practices," 2024. https://www.dataprise.com/resources/blog/healthcare-best-cybersecurity-practices/
[39] DigiCert, "How Will Quantum Computing Impact Healthcare Security?," 2023. https://www.digicert.com/blog/how-will-quantum-computing-impact-healthcare-security
[40] DigiKey, "Low-Power MCUs Simplify Healthcare and IIoT Design," 2025. https://www.digikey.com/en/articles/use-a-portfolio-of-microcontrollers-for-healthcare-industrial-iot-design
[41] Eastgate Software, "Blockchain for Data Security in Mobile Health Applications," *Journal of Medical Blockchain Research*, vol. 15, no. 2, pp. 34–51, 2025.
[42] Eastgate Software, "Cybersecurity in Healthcare: Protecting Patient Data and Systems," 2025. https://eastgate-software.com/cybersecurity-in-healthcare-protecting-patient-data-systems/
[43] EICTA, "IoT Networks: Communication Protocols, Security, and Infrastructure," 2022. https://eicta.iitk.ac.in/knowledge-hub/internet-of-things/iot-networks-communication-protocols-security-and-infrastructure/
[44] eInfochips, "Importance of Cybersecurity in Healthcare and Medical Devices," 2022. https://www.einfochips.com/blog/importance-of-cybersecurity-in-healthcare-and-medical-devices/
[45] A. Faraone and R. Delgado-Gonzalo, "Convolutional-Recurrent Neural Networks on Low-Power Wearable Platforms for Cardiac Arrhythmia Detection," *arXiv preprint*, 2020. https://doi.org/10.1109/AICAS48895.2020.9073950
[46] S. Frey, M. Guermandi, S. Benatti, V. Kartsch, A. Cossettini, and L. Benini, "BioGAP: a 10-Core FP-capable Ultra-Low Power IoT Processor, with Medical-Grade AFE and BLE Connectivity for Wearable Biosignal Processing," *arXiv preprint*, 2023. https://doi.org/10.1109/COINS57856.2023.10189286
[47] Frontegg, "7 Multi-Factor Authentication Solutions and Their Pros/Cons," 2023. https://frontegg.com/guides/multi-factor-authentication-solutions

[48] GE HealthCare, "Cybersecurity in Healthcare: Connectivity of Medical Devices," 2023. https://www.gehealthcare.com/insights/article/cybersecurity-in-healthcare-connectivity-of-medical-devices
[49] Healthcare Tech Outlook, "The Importance of Cybersecurity in Protecting Patient Safety," 2024. https://www.healthcaretechoutlook.com/news/the-importance-of-cybersecurity-in-protecting-patient-safety-nid-4257.html
[50] B. Inkster, C. Knibbs, and M. Bada, "Cybersecurity: a Critical Priority for Digital Mental Health," Frontiers in Digital Health, vol. 5, 2023. https://doi.org/10.3389/fdgth.2023.1242264
[51] W. Jack, "Mobile Health and IoT Security: A Threat Modeling Approach to Enhance Cyber Security and Ensure Corporate Resilience," *ResearchGate*, 2024. https://www.researchgate.net/publication/387502162_Mobile_Health_and_IoT_Security
[52] M. A. Khan and K. Salah, "Hybrid Lightweight Cryptography Using AES and ECC for IoT Security," *Advances in Intelligent Systems and Computing*, vol. 1365, pp. 213–223, 2022. https://link.springer.com/chapter/10.1007/978-981-99-9811-1_19
[53] A. Knight, "100% of Tested mHealth Apps Vulnerable to API Attacks," *HIPAA Journal*, 2021. https://www.hipaajournal.com/100-of-tested-mhealth-apps-vulnerable-to-api-attacks/
[54] M. Kosinski, "What is a Data Breach," 2024. https://www.ibm.com/topics/data-breach
[55] N. Kshetri, R. Mishra, M. M. Rahman, and T. Steigner, "HNMblock: Blockchain Technology Powered Healthcare Network Model for Epidemiological Monitoring, Medical Systems Security, and Wellness," *arXiv preprint*, 2024.
[56] M. Kumar, H. Raj, N. Chaurasia, and S. S. Gill, "Blockchain Inspired Secure and Reliable Data Exchange Architecture for Cyber-Physical Healthcare System 4.0," *arXiv preprint*, 2023.
[57] LifeWire, "Microsoft Outages Show Why Governments Need to Ditch Big Tech," 2024. https://doi.org/10.1016/j.iotcps.2023.05.006
[58] T. Lu, "A Survey on RISC-V Security: Hardware and Architecture," *arXiv preprint*, 2021. https://arxiv.org/abs/2107.04175
[59] S. O. Maikol, A. S. Khan, Y. Javed, A. L. A. Bunsu, C. Petrus, H. George, and S. Jau, "A Novel Authentication and Key Agreement Scheme for Countering MITM and Impersonation Attack in Medical Facilities," *International Journal of Integrated Engineering*, vol. 13, no. 2, pp. 127–135, 2021. https://doi.org/10.30880/ijie.2021.13.02.015
[60] J. Martinez and J. McCarthy, "What is an Attack Vector? 15 Common Attack Vectors to Know," 2024. https://www.strongdm.com/blog/attack-vector
[61] mHealth Hub, "Cybersecurity in the Future of Health," 2024. https://mhealth-hub.org/cybersecurity-in-the-future-of-health
[62] Microsoft, "TPM Recommendations," 2023. https://learn.microsoft.com/en-us/windows/security/hardware-security/tpm/tpm-recommendations
[63] MoldStud, "Best Practices for Maintaining Security During Software Updates in Custom Software," 2025. https://moldstud.com/articles/p-effective-strategies-for-ensuring-security-throughout-the-software-update-process-in-custom-applications
[64] D. H. Morais, "Data Communication Systems Protocol Stacks," *5G/5G-Advanced, Wi-Fi 6/7, and Bluetooth 5/6. Cham: Springer*, 2025. https://doi.org/10.1007/978-3-031-82830-0_2
[65] S. M. Mousavi, A. Zekry, and H. Patel, "Cybersecurity Risks and Countermeasures for Medical IoT Devices: An Embedded Systems Perspective," *Journal of Medical Systems*, vol. 47, no. 2, pp. 29, 2023. https://doi.org/10.1007/s10916-023-1903-8
[66] Mousavi et al., "Cyber Threats and Countermeasures in Embedded Medical Devices," *IEEE Transactions on Biomedical Engineering*, vol. 70, no. 4, pp. 1230–1245, 2023.
[67] National Institute of Standards and Technology (NIST), "Guidelines for Medical Device Security in Healthcare Settings," *NIST Special Publication 800-82 Rev. 3*, 2024. https://doi.org/10.6028/NIST.SP.800-82r3
[68] NBC Chicago, "The Foundation of Modern Software Development is Under Rising Cyber Attack," 2024. https://www.nbcchicago.com/news/business/money-report/the-foundation-of-modern-software-development-is-under-rising-cyber-attack/3675442/
[69] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "A Survey on Security and Privacy Issues in Modern Healthcare Systems," AC*M Transactions on Computing for Healthcare*, vol. 2, no. 3, 2021. https://doi.org/10.1145/3453176
[70] L. H. Newman, "Therapy Sessions Exposed by Mental Health Care Firm's Unsecured Database," *Wired*, 2024. https://www.wired.com/story/confidant-health-therapy-records-database-exposure
[71] NXP Semiconductors, "Post-Quantum Cryptography: Migration Challenges for Embedded Devices," 2024. https://www.nxp.com/docs/en/white-paper/POSTQUANCOMPWPA4.pdf
[72] Openware, "Blockchain in Healthcare: Improving Data Security and Patient Privacy," 2023. https://www.openware.com/news/articles/blockchain-in-healthcare-improving-data-security-and-patient-privacy
[73] OriginStamp, "The Cybersecurity Risks of Using Outdated Software," 2022. https://originstamp.com/blog/the-cybersecurity-risks-of-using-outdated-software
[74] D. Papp, Z. Ma, and L. Buttyán, "Embedded Systems Security: Threats, Vulnerabilities, and Attack Taxonomy," *Proceedings of the 13th Annual Conference on Privacy, Security and Trust (PST)*, pp. 145–152, 2015. https://doi.org/10.1109/PST.2015.7232966
[75] Ping I., "The Imperative of Multi-Factor Authentication (MFA) in Healthcare," 2023. https://www.pingidentity.com/en/resources/blog/post/imperative-mfa-in-healthcare.html

[76] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, "Analyzing the Energy Consumption of Security Protocols," *Proceedings of the 2003 International Symposium on Low Power Electronics and Design*, pp. 30–35, 2003. https://doi.org/10.1145/871506.871518
[77] M. Prakash, "The CIA Triad (Confidentiality, Integrity, and Availability)," 2022. https://www.knowledgehut.com/blog/security/cia-in-cyber-security
[78] PUFsecurity, "TPM 2.0-Ready: Top Security with PUFcc,". https://www.pufsecurity.com/document/tpm-2-0-ready-top-security-with-pufcc/
[79] Quantinuum, "Quantinuum," 2024. https://en.wikipedia.org/wiki/Quantinuum
[80] M. M. Rahman, S. Kabir, and I. H. Sarker, "AI-Driven Anomaly Detection in Healthcare IoT Networks: Strengthening Cybersecurity Against Threats," *Future Generation Computer Systems*, vol. 140, no. 4, pp. 150–165, 2023. https://doi.org/10.1016/j.future.2023.08.015
[81] Reinvently, "Ensuring HIPAA Compliance in Mobile Health Apps," *Health Tech Compliance Review*, vol. 9, no. 1, pp. 22–40, 2017.
[82] Renesas, "High Data Throughput using Bluetooth® Low Energy for Low-Power Wireless Communication," 2019. https://www.renesas.com/us/en/document/whp/high-data-throughput-using-bluetooth-low-energy-low-power-wireless-communication
[83] R. Sahay, J. P. Mishra, and S. K. Sahay, "Modern Hardware Security: A Review of Attacks and Countermeasures," *arXiv preprint*, 2025. https://arxiv.org/abs/2501.04394
[84] A. H. Seh, M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal, R. Kumar, and R. A. Khan, "Healthcare Data Breaches: Insights and Implications," Healthcare (Switzerland), vol. 8, no. 2, 2020. Link: https://doi.org/10.3390/healthcare8020133
[85] SEI Blog, "Secure Software Updates," 2016. https://insights.sei.cmu.edu/blog/secure-software-updates/
[86] M. A. Siddiqi, C. Doerr, and C. Strydis, "IMDfence: Architecting a Secure Protocol for Implantable Medical Devices," *arXiv preprint*, 2020. https://doi.org/10.1109/ACCESS.2020.3015686
[87] R. Singh and P. Gupta, "Artificial Intelligence for Threat Detection in Healthcare Cybersecurity," *AI & Healthcare Security Journal*, vol. 19, no. 1, pp. 89–102, 2024.
[88] R. Singh and P. Gupta, "Enhancing Security in Smart Healthcare: A Framework for Resilient Embedded Systems," *IEEE Transactions on Biomedical Engineering*, vol. 71, no. 1, pp. 77–89, 2024. https://doi.org/10.1109/TBME.2024.3289762
[89] D. Stewart and I. Approov, "The Mobile Attack Pyramid: Identifying Attack Surfaces is Key to Protecting Mobile Applications," 2021. https://www.cyberdefensemagazine.com/the-mobile-attack-pyramid/
[90] The Verge, "The US Proposes Rules to Make Healthcare Data More Secure," 2024. https://www.theverge.com/2024/12/28/24330878/the-us-proposes-rules-to-make-healthcare-data-more-secure
[91] Y. Xing, H. Lu, L. Zhao, and S. Cao, "Privacy and Security Issues in Mobile Medical Information Systems," *Mobile Networks and Applications*, vol. 29, pp. 762–773, 2024. https://doi.org/10.1007/s11036-024-02299-8
[92] Z. Xu, Y. Hao, A. Luo, and Y. Jiang, "Technologies and Applications in Wireless Biosensors for Real-Time Health Monitoring," *Med-X*, vol. 2, art. no. 24, 2024. https://doi.org/10.1007/s44258-024-00041-3
[93] A. A. Yavuz, S. Darzi, and S. E. Nouma, "Lightweight and Scalable Post-Quantum Authentication for Medical Internet of Things," *arXiv preprint*, 2023. https://arxiv.org/abs/2311.18674
[94] J. Yttri, W. Nilsen, and S. Arora, "Privacy and Security in Mobile Health (mHealth) Research," 2014. http://www.ecfr.gov/cgi-bin/
[95] Zac A., "Security Risks of Biometric Authentication in mHealth," 2025. https://thejournalofmhealth.com/security-risks-of-biometric-authentication-in-mhealth/