BILINGUAL PUBLISHING GROUP

Journal of Electronic & Information Systems

https://journals.bilpubgroup.com/index.php/jeis

REVIEW

Review of Embedded Systems and Cyber Threat Intelligence for Enhancing Data Security in Mobile Health

Anayo Chukwu Ikegwu [1,2*], ***Victoria Chibuzo Uzuegbu*** [3], ***Uzoma Rita Alo*** [1]

[1]*Computer Science Department, Faculty of Physical Sciences, Alex Ekwueme Federal University Ndufu-Alike, Abakaliki P.M.B. 1010, Nigeria*

[2]*Software Engineering Department, Faculty of Natural and Applied Sciences, Veritas University Abuja, Abuja 901101, Nigeria*

[3]*Computer Science Department, Faculty of Natural and Applied Sciences, Veritas University Abuja, Abuja 901101, Nigeria*

ABSTRACT

Embedded systems play a vital role in mobile health (mHealth) by enabling real-time health monitoring and personalized care through devices like wearables and sensors. However, these systems handle sensitive health data, making them vulnerable to cyber threats such as data breaches and unauthorized access. Traditional security measures are often inadequate against evolving attacks, raising concerns over data safety. This paper reviews how cyber threat intelligence (CTI) can be integrated with embedded systems in mHealth to enhance security. CTI provides real-time insights into potential threats, enabling proactive detection and prevention through tools like intrusion detection systems and predictive analytics. The study examines current embedded system applications in mHealth, associated security challenges, and how CTI strengthens security frameworks. It emphasizes the need for specialized CTI models and collaborative threat intelligence sharing in the healthcare sector. We further provided a practical examples and case studies to showcase the application of CTI in securing embedded systems within mHealth environments. The key findings demonstrate CTI's effectiveness in safeguarding vital health data and guiding future innovations in healthcare cybersecurity. The implications of this study would enhance data security, establish uniform security policies, and facilitate the growth of mHealth technology for effective development of optimal healthcare services by the practitioner, policymakers, medical health developers.

Keywords: Embedded Systems; Cyber Threat Intelligence; Data Security; Mobile Health; Internet of Things; Healthcare Patient Data

*CORRESPONDING AUTHOR:

Anayo Chukwu Ikegwu, Computer Science Department, Faculty of Physical Sciences, Alex Ekwueme Federal University Ndufu-Alike, Abakaliki P.M.B. 1010, Nigeria; Email: ikegwua@veritas.edu.ng

ARTICLE INFO

Received: 8 February 2025 | Revised: 17 March 2025 | Accepted: 27 March 2025 | Published Online: 5 April 2025

DOI: https://doi.org/10.30564/jeis.v7i1.10050

CITATION

Ikegwu, A.C., Uzuegbu, V.C., Alo, U.R., 2025. Review of Embedded Systems and Cyber Threat Intelligence for Enhancing Data Security in Mobile Health. Journal of Electronic & Information Systems. 7(1): 98–120. DOI: https://doi.org/10.30564/jeis.v7i1.10050

1. Introduction

Maintaining good health and the security of personal information is vital in the contemporary environment. Mobile health, or mHealth, refers to the provision of healthcare services via mobile devices, such as wearables, tablets, and smartphones [1] . As mobile technology has advanced, mHealth, which enables remote monitoring, telemedicine, and health tracking, has become an essential part of modern healthcare systems. Specifically, the integration of mHealth devices with healthcare systems has enabled real-time tracking of patient conditions, leading to better patient outcomes and lower healthcare costs [2-3]. Furthermore, wearable technology, like fitness trackers, allows users to continuously monitor their health metrics and is increasingly being used for individualized health management.

Consequently, the role of embedded systems in mHealth becomes paramount. Real-time data processing and control are made possible by embedded systems, which are the foundation of mobile health devices. Indeed, the sensors that these systems are designed to interface with monitor blood pressure, glucose levels, heart rate, and other health parameters. Therefore, for mHealth devices to be portable and have a longer battery life, embedded systems must use little electricity [4]. Moreover, embedded systems are critical for remote patient monitoring and diagnostics because they help ensure the accuracy and reliability of patient data.

Given the sensitive nature of the data handled by these embedded systems, the importance of data security in mHealth cannot be overstated. Due to the sensitive nature of data, especially health data, robust data security measures are required to prevent breaches and unauthorized access [5]. Notably, since mHealth devices collect and transmit private data, including biometric data, personal identifiers, and medical histories, they are frequently the target of cyberattacks [6-7]. In turn, healthcare data breaches have major consequences, such as identity theft, financial loss, and a decline in patient trust in healthcare providers. Therefore, securing mHealth devices is necessary to safeguard the privacy and security of patients and healthcare providers from such assaults.

To effectively address these security challenges, Cyber Threat Intelligence (CTI) is essential. Cyber Threat Intelligence (CTI) collects, analyzes, and disseminates information regarding potential cyber threats. Crucially, by integrating CTI into mHealth systems, it is now possible to predict, detect, and mitigate emerging cybersecurity risks. In essence, CTI helps businesses keep ahead of attackers by identifying weaknesses in networks or devices and analyzing trends in malicious activity. For example, CTI can be used in mHealth to find anomalies in how devices are operating or unauthorized attempts to obtain private health data [8]. Ultimately, by using CTI, mHealth systems can proactively defend against attacks and mitigate the effects of cyber risks.

1.1. Related Work

The increasing prevalence of mobile health (mHealth) applications has introduced significant cybersecurity challenges, necessitating robust security measures within embedded systems. While existing research has explored various security enhancements, the dynamic integration of Cyber Threat Intelligence (CTI) for proactive threat mitigation in mHealth remains a relatively underexplored area. Several studies have focused on leveraging Artificial Intelligence (AI) for intrusion detection and security enhancement in related domains. For example, [9] explored advanced cybersecurity strategies for health management systems, including IoMT security frameworks, blockchain, and AI. They reported a 97% reduction in unauthorized access attempts through blockchain implementation. While this study demonstrates the efficacy of AI and blockchain in enhancing security, it does not specifically address the integration of CTI within embedded systems for real-time threat adaptation. Furthermore, [10] highlighted the significance of AI in improving threat intelligence for healthcare cybersecurity. Their research emphasizes the use of data analytics and machine learning for real-time threat detection and response. However, the practical implementation of CTI within the resource-constrained environment of embedded systems in mHealth applications has not been thoroughly investigated. Broader reviews, such as [11], have examined cybersecurity interventions in healthcare organizations, emphasizing the importance of organizational and cultural factors like staff training and regulatory compliance. While crucial, these studies do not delve into the

technical specifics of integrating CTI into embedded systems. Recent developments, such as the collaboration between MediaTek and Exein have focused on incorporating cybersecurity safeguards at the chip level. This initiative aims to improve device security by embedding security measures directly into processors. However, it does not explicitly address the dynamic and adaptive nature of CTI integration required to counter evolving cyber threats in mHealth. In contrast to these studies, this research focuses on the dynamic integration of CTI into the embedded systems of mHealth applications. By enabling proactive, real-time attack identification and mitigation, this approach aims to address the unique and evolving cybersecurity challenges specific to the mHealth domain. This study will explore methods to efficiently incorporate CTI into embedded systems, considering the resource constraints and real-time requirements of mHealth applications, thereby providing a more resilient and adaptive security framework.

1.2. The Objective of the Review

This paper aims to explore how integrating Cyber Threat Intelligence (CTI) into embedded systems can enhance the data security of mHealth devices. The review will focus on real-time threat detection, prediction, and response while examining the potential benefits and challenges of this integration. The primary goal is to demonstrate how CTI can ensure the continued dependability of these essential medical devices, protect private health information, and enhance the resilience of mHealth devices against evolving cyber threats.

This study examines the crucial relationship between data security, embedded systems, and Cyber Threat Intelligence (CTI) in the context of mobile health (mHealth) having the following specific contribution to the body knowledge.

- A comprehensive examination of embedded systems, CTI, and the specific data security concerns prevalent in mHealth were provided.
- We explored the methodologies through which CTI can effectively enhance the security of embedded systems in mHealth.
- We further provided practical examples and case studies to showcase the application of CTI in securing embedded systems within mHealth environments.
- We provided the descriptions, strengths, and weaknesses of mHealth embedded systems, the architecture of embedded systems in mHealth, and solutions in securing embedded systems.

We also provided the techniques, description, strengths, and weaknesses for enhancing data security in mHealth using embedded systems.

2. Embedded Systems in Mobile Health

Mobile health apps use embedded technologies to track a number of health metrics, such as blood pressure, heart rate, blood sugar, and physical activity. To give full health data, these applications frequently interact with wearable technology, such as activity trackers and smartwatches. Timely interventions and customized treatment plans are made possible by the transmission of the gathered data to cloud-based platforms or healthcare providers for [12-13]. The effectiveness of transmitting health data has also increased with the use of body area networks (BANs). Wearable technology that gathers health data and wirelessly connects to other gadgets or healthcare systems makes up BANs. Numerous applications, such as chronic disease management and remote patient monitoring, have made use of this technology [13]. The possibilities of mHealth applications have been improved by recent developments in embedded systems. The creation of connected health devices that provide real-time monitoring and data analysis has been made easier by the incorporation of the Internet of Medical Things (IoMT). The design and modeling of smart health monitoring systems, for example, are covered in a 2023 study that emphasizes the function of embedded systems in facilitating ongoing data collecting and health monitoring [13]. The possibilities of mHealth applications have been improved by recent developments in embedded systems. The creation of connected health devices that provide real-time monitoring and data analysis has been made easier by the incorporation of the Internet of Medical Things (IoMT). The design and modeling of smart health monitoring systems, for example, are covered in a 2023 study that emphasizes the function of embedded systems in facilitating ongoing data collecting and health monitoring [13]. The integration of embedded systems in mHealth

still faces several obstacles, notwithstanding the progress made. Since sensitive health information is transferred and kept digitally, protecting patient privacy and data security is crucial. Furthermore, to guarantee efficient healthcare delivery, the precision and dependability of health data gathered by embedded systems must be confirmed. According to [14], a thorough analysis of mobile healthcare applications highlights the essential problems and difficulties in system design, such as data security and system dependability.

2.1. Major Components of Mobile Health Embedded Systems

(i) Sensors: Gathering Information about Patients' Heart rate, blood pressure, temperature, and glucose levels is just a few of the health-related data that sensors in mHealth devices gather. These sensors include devices like accelerometers, pulse oximeters, and electrocardiogram (ECG) sensors [15]. They provide real-time data for diagnosis and treatment by continuously monitoring the patient's physiological characteristics, making educated healthcare decisions and facilitating individualized care depending on the data gathered by these sensors [16].

(ii) Microcontrollers and Processors: In handling the processing of Data, Microcontrollers and processors are the brains of embedded systems; they are in charge of gathering, processing, and reporting sensor data. These elements need to be energy-efficient and able to process data in real time, which is crucial for mHealth applications like fall detection and heart rate monitoring that need quick reactions. Since they are efficient in terms of power consumption and computing capability, ARM-based processors and low-power microcontrollers are commonly utilized [17].

(iii) Communication Modules: For mHealth devices to send data for remote monitoring, connectivity must be enabled. This transmission is made possible via communication modules including Bluetooth, Wi-Fi, and 4G/5G technologies. While Wi-Fi is utilized for cloud-based storage and larger data sets, Bluetooth is frequently employed for short-range communication, enabling devices to connect with smartphones for data transmission. High-volume, real-time data transmission is made possible by 4G and 5G technologies, which are helpful in vital healthcare applications [18].

The descriptions, strengths, and weaknesses of mHealth-embedded systems are presented in **Table 1**.

Table 1. Descriptions, Strengths, and Weaknesses of mHealth Embedded Systems.

System components	Description	Strengths	Weaknesses	References
Sensors	Collect health-related data (e.g., heart rate, BP, temperature, glucose).	Real-time monitoring supports individualized care	Accuracy may vary; sensor drift	[15-16],
Microcontrollers/ Processors	Process and manage sensor data; enable real-time decision-making.	Energy efficient; suitable for real-time processing	Limited computational power	[17]
Communication Modules	For remote access and monitoring, data can be transmitted via Bluetooth, Wi-Fi, or 4G/5G.	Enables real-time data sharing; supports mobility	Connectivity issues, power consumption	[18]
Sensors	Collect health-related data (e.g., heart rate, BP, temperature, glucose).	Real-time monitoring supports individualized care	Accuracy may vary; sensor drift	[15-16],
Microcontrollers/ Processors	Process and manage sensor data; enable real-time decision-making.	Energy efficient; suitable for real-time processing	Limited computational power	[17]

2.2. Architecture of Embedded Systems in Mobile Health

The embedded system architecture in mobile health (mHealth) devices is made to effectively collect, process, and send health data in real time while using the least amount of power possible. The framework usually consists of several essential parts that cooperate to support the

operation of medical monitoring equipment. They can be grouped into four main layers:

(i) Sensing Layer: In mHealth systems, the sensing layer is the fundamental layer. It comprises the different sensors that are built into wearable medical equipment and gather information from the user. Physiological characteristics like heart rate, body temperature, glucose levels, and mobility data are all measured by sensors. Depending on the gadget and its intended use, many kinds of sensors may be employed. Photoplethysmography (PPG) sensors gauge blood oxygen saturation (SpO2) and heart rate. Gyroscopes and accelerometers: track posture, movement, and physical activity. Temperature sensors: track the temperature of the body. Electrocardiogram (ECG) sensors: These are utilized in cutting-edge wearable medical equipment to continuously monitor the heart [19].

(ii) Processing Layer: The microcontroller/processor, which controls the data processing, is the central component of the embedded system. Interpreting sensor input, carrying out required computations, and getting the data ready for transmission to the following layer are the responsibilities of this layer. This layer is made up of,

(1) *Microcontrollers (MCUs):* tiny, low-power processors that govern how the device works. These MCUs regulate power usage, process sensor data, and execute firmware for real-time monitoring. Microcontrollers used in mHealth devices are tuned for energy efficiency, and these devices are frequently made to be portable and have long battery lives. This guarantees that gadgets like smartwatches and fitness trackers may function for prolonged periods between charges.

(2) *Signal Processing Units:* To generate valuable health insights, specialized processors may be utilized in gadgets such as ECG monitors to filter and analyze raw sensor data [20].

(iii) Communication Layer: Data flow between the embedded system and external devices, such as cloud servers and cell phones, is made possible via the communication layer. Commonly employed for this purpose are wireless communication technologies like Bluetooth, Wi-Fi, and cellular networks (4G/5G). For instance, for short-range communication, such as sending data from a smartwatch to a smartphone app, Bluetooth is utilized. Wi-Fi: Enables faster data transfer to cloud systems, facilitating more thorough analysis and archiving of health data. Cellular Networks (4G/5G): These networks are utilized in gadgets such as remote health monitors to share data in real-time with medical professionals, allowing for remote patient monitoring. The communication layer also supports secure data transmission, which is critical to ensure patient privacy and comply with regulatory standards like HIPAA (Health Insurance Portability and Accountability Act) in the United States [21].

(iv) Application Layer: Based on the processed data, the application layer communicates with the end user and offers insightful comments. This layer consists of mobile apps that let users see their health information and get warnings or notifications based on their current condition. Cloud platforms: These allow healthcare practitioners to remotely monitor patient status by storing, analyzing, and exchanging health data. User Interface (UI): A crucial component of usability, allowing users to engage with the gadget and get feedback via vibrations, noises, or visual cues [22].

The descriptions, strengths, and weaknesses of the architecture of embedded systems in mHealth are presented in **Table 2**.

Table 2. Descriptions, Strengths, and Weaknesses of the Architecture of Embedded Systems in mHealth.

Architecture	Description	Strengths	Weaknesses	References
Sensing Layer	Collects raw data from sensors (e.g., ECG, temperature, accelerometers).	Real-time and continuous monitoring	Sensor limitations: environmental interference	[19]
Processing Layer	Microcontrollers and signal processors for local computation.	Low power, fast response time	Limited processing power	[20]
Communication Layer	Transfers data wirelessly via Bluetooth, Wi-Fi, or cellular networks.	Enables remote monitoring; secure transfer	Vulnerable to attacks; requires network access	[22]
Application Layer	Provides feedback and interface to users via apps or cloud platforms.	User engagement supports remote access	Usability challenges, privacy risks	[22]

2.3. mHealth Devices

To track and control health, many mHealth devices use embedded systems. Popular examples are smartwatches like the Apple Watch and Fitbit, which give consumers constant tracking of blood oxygen levels, heart rate, steps, and sleep. These gadgets process sensor data and send it to smartphones for additional analysis via embedded systems [23].

(i) Wearable Devices: Continuous glucose monitors (CGMs) and ECG patches are two examples of wearable health monitoring devices. Continuously monitoring a patient's health, these gadgets notify users or medical professionals of any abnormal readings. Additionally, embedded systems are used for data gathering and processing in mobile diagnostic equipment, including blood pressure cuffs or handheld ultrasound machines, which provide results that may be sent right away to a medical practitioner [24].

(ii) Smartwatches Devices: Devices such as the Fitbit and Apple Watch have gained popularity as tools for ongoing health monitoring. These gadgets interpret data from sensors like accelerometers and heart rate monitors using embedded systems to give users real-time feedback on their health parameters. For in-depth examination, the data is frequently synced to mobile apps [25].

(iii) Mobile Diagnostic Devices: People can monitor their health concerns at home with portable diagnostic devices, such as ECG monitors. These gadgets utilize embedded systems to collect, process, and transmit data in real-time to healthcare providers [26-27].

The device type, function, examples, strengths, and weaknesses of mhealth devices are presented in **Table 3**.

Table 3. Device Type, Function, Examples, Strengths, and Weaknesses of mHealth Devices.

Device Type	Function	Examples	Strengths	Weaknesses	References
Wearable Devices	Monitor vital signs continuously (e.g., CGMs, ECG patches).	Freestyle Libre, Zio Patch	Continuous monitoring	Cost: user training	[24]
Smartwatches	Track health metrics via embedded sensors (heart rate, activity, SpO_2).	Apple Watch, Fitbit	Multi-functional, user-friendly	Battery life, sensor limitations	[25]
Mobile Diagnostic Devices	Provide spot-check measurements at home (e.g., BP cuffs, portable ECGs).	Kardia Mobile, Qardio Arm	Convenient, real-time alerts	Limited diagnostic scope	[26-27].

2.4. Challenges in Securing Embedded Systems

The integration of embedded systems into medical devices presents several challenges and concerns, particularly concerning interoperability standardization and cybersecurity risks. Cybersecurity risks include the potential for remote hacking and data breaches, which jeopardize patient privacy [28]. As medical devices become more linked to healthcare IT networks, their vulnerability to cyberattacks increases, raising concerns about the security of patient data and the potential for remote medical device manipulation [29].

In order to resolve compatibility issues and provide a seamless device connection, standardized interoperability is also crucial [30]. Interoperability is hampered by the variability of medical equipment from different vendors, while data transmission between devices is still being researched and defined [31]. The FDA's ability to evaluate the safety and effectiveness of medical devices in the US has been confirmed by the Medical Device Amendments Act [32]. Yet, Sonko, Monebi, Etukudoh, Osasona, Atadoga, and Daudu have observed that medical devices are becoming increasingly integrated with modern computer networks. [33] state that standards for medical device interoperability must be developed for medical information systems to communicate across organizational, system, and regional boundaries. The use of embedded systems in medical devices raises some concerns and challenges, including cybersecurity risks and standardization of interoperability. To ensure the safety, security, and seamless operation of medical equipment inside healthcare systems, these issues need to be resolved. Because they must function continuously,

have limited resources, and require real-time processing, embedded systems in mHealth devices provide special security challenges. Conventional security solutions are challenging to apply in embedded systems because they frequently have low memory and little processing capacity, in contrast to standard computing platforms, which have strong hardware capabilities and comprehensive security frameworks [34]. The following are the main obstacles to embedded system security in mHealth applications.

2.4.1. Limited Computational Power and Resource Constraints

The restricted processing power and memory limitations of embedded devices present a significant security concern. Embedded systems, in contrast to general-purpose computers, are made to carry out certain tasks while using the least amount of power possible. Low-power embedded devices might not be able to handle computationally demanding procedures needed for security measures, including encryption, intrusion detection systems, and real-time monitoring [35]. Furthermore, because cryptographic processes can rapidly deplete battery life, the requirement to maximize battery life in wearable health devices further restricts the application of conventional security algorithms [36].

2.4.2. Real-Time Data Processing Requirements

To guarantee prompt and precise patient monitoring, mHealth devices must process data in real time. For instance, data processing and transmission to healthcare providers must happen instantly for wearable devices that monitor glucose levels or heart rate. Complex encryption algorithms and other strong security measures can cause processing delays, which can be harmful in time-sensitive applications. For this reason, security solutions must be created that strike a balance between strong protection against cyber threats and real-time responsiveness [37].

2.4.3. Lack of Regular Security Updates and Patch Management

Embedded systems in mHealth devices sometimes run on static firmware that is not updated frequently, in contrast to current computing devices that receive regular software updates and security fixes. Because hackers can take advantage of out-of-date firmware with known vulnerabilities, they are exposed to both zero-day and long-term security threats [38]. Limited connectivity, the intricacy of firmware upgrades, and the possibility of interfering with device operation when upgrading are some of the reasons why updating embedded systems can be challenging [39].

2.4.4. Vulnerability to Physical and Network Attacks

mHealth devices are vulnerable to network-based and physical attacks. Through physical access, an attacker can change firmware, remove private information, or get around security measures on an embedded device. Network-based threats, like man-in-the-middle (MitM) attacks, can intercept data transfers between healthcare servers and mHealth devices, resulting in data breaches and illegal access. To compromise device security, attackers can take advantage of poor authentication procedures or unencrypted data transmissions, as many embedded systems depend on wireless connections (e.g., Bluetooth, Wi-Fi, or cellular networks) [16].

2.4.5. Integration Challenges with Cyber Threat Intelligence

Real-time threat detection and response methods are two ways that Cyber Threat Intelligence (CTI) might improve embedded system security. However, there are several obstacles to overcome when incorporating CTI into embedded devices with limited resources, as real-time threat intelligence processing requires computing power and storage capacity that these devices often lack. Furthermore, network access is necessary for ongoing cyber threat monitoring and analysis, which may not always be possible for embedded devices functioning in remote healthcare settings [40].

The challenges, descriptions, and solutions in securing embedded systems are shown in **Table 4**.

Table 4. Challenges, Descriptions, and Solutions in Securing Embedded Systems.

Challenges	Description	Solutions	References
Limited Computational Power	Embedded systems lack the power for complex encryption/security tasks.	Use lightweight cryptographic algorithms; offload tasks to hardware modules	[35-36]
Real-Time Processing Needs	Strong encryption may delay time-sensitive monitoring.	Design low-latency security protocols	[37]
Lack of Regular Updates	Infrequent firmware updates increase the risk of exploits.	Implement OTA (over-the-air) updates; secure firmware management	[38-39]
Network & Physical Attack Exposure	Devices are prone to MitM attacks and physical tampering.	Secure boot, strong encryption, and authentication protocols	[16]
CTI Integration Limitations	Devices may not handle real-time threat intelligence due to resource constraints.	Integrate only essential CTI; use edge-assisted monitoring	[40]
Interoperability Standardization	Devices from different vendors may not communicate seamlessly.	Enforce global standards and cross-platform frameworks	[30-31]
Limited Computational Power	Embedded systems lack the power for complex encryption/security tasks.	Use lightweight cryptographic algorithms; offload tasks to hardware modules	[35-36]
Real-Time Processing Needs	Strong encryption may delay time-sensitive monitoring.	Design low-latency security protocols	[37]

3. Methodology

3.1. Research Design

This study uses a qualitative review methodology to investigate the function of embedded systems and the security implications of mHealth applications. Understanding how cyber threat intelligence (CTI) can improve these systems' security is the main goal of the review. The methodology employs a methodical approach to collect and evaluate data from the body of current research, evaluating the potential for CTI integration as well as the state of the art in mHealth security.

3.2. Data Collection

To ensure transparency and reproducibility, a systematic literature review approach was adopted for the data collection process. This involved a well-defined protocol that included database selection, keyword formulation, time frame, and inclusion/exclusion criteria.

(i) Databases Searched: The literature search was conducted using the following major academic and technical databases to ensure broad coverage of both scientific and industry-related research: IEEE Xplore, PubMed, SpringerLink, ScienceDirect, and Google Scholar. These databases were chosen based on their relevance to engineering, medical, and cybersecurity disciplines.

(ii) Search Terms Used: Search queries were developed to target literature at the intersection of embedded systems, mHealth, and cybersecurity. The following keywords and Boolean combinations were used: Embedded systems in mobile health, mHealth security, cyber threat intelligence and mHealth, data protection in mobile health applications, security protocols in wearable health technology, CTI and embedded medical devices, and searches were conducted using these combinations to capture both broad and specific results.

(iii) Time Frame: The review focused on literature published between 2013 – 2025, reflecting the current technologies and trends.

(iv) Inclusion Criteria: Studies were selected based on the following criteria: Peer-reviewed journal articles, reputable conference proceedings, industry reports, and white papers, research involving embedded system architectures, CTI methods, and cybersecurity mechanisms in mHealth, papers discussing implementation, case studies,

or evaluations of real-world mHealth applications, and English-language publications only.

(v) Exclusion Criteria: The following types of publications were excluded: Articles published before 2013, papers not available in full text, studies focusing solely on general healthcare IT without relevance to embedded systems or CTI.

(vi) Screening and Selection Process: Initial screening: Titles and abstracts of search results were reviewed for relevance.

- Full-text review: Selected articles underwent a detailed full-text evaluation to ensure alignment with the research objectives.
- Reference checking: References of included studies were manually reviewed to identify additional relevant sources.

3.3. Data Analysis

Two levels of analysis were conducted:

i. Descriptive Analysis: Studies were categorized based on focus areas (e.g., embedded architectures, CTI strategies, mHealth case studies).

ii. Thematic Analysis: Findings were compared across case studies to understand patterns in security implementation and CTI effectiveness.

3.4. Framework Development

The insights from the literature review are used to construct a conceptual framework. This framework describes. The essential elements of embedded mobile health systems and the dangers and hazards that might compromise the security of the data in these systems.

4. Cybersecurity Threats in mHealth Systems

Cybercriminals increasingly target mobile health (mHealth) systems, which use mobile devices and apps to manage health data. Securing these systems is essential to guarantee the safety and privacy of patient data as healthcare increasingly depends on digital platforms. Organizations need to handle many common dangers to mHealth systems. The sophistication and frequency of cyberattacks will increase with the ongoing evolution of healthcare systems. mHealth systems must constantly upgrade their cybersecurity frameworks to protect against changing threats because of the advent of more sophisticated cybercriminal strategies, including the use of AI for more focused and effective attacks. Applications for mobile health (mHealth) are becoming more vulnerable to cybersecurity risks since they integrate with several devices and transmit private health information. To address these issues, several researchers have put forth theories, tactics, and algorithms to improve security in mHealth settings. The following are some noteworthy instances:

(i) *MSF*: A Comprehensive Security Framework for mHealth Applications. A security architecture intended to handle privacy and security concerns in mHealth applications is presented in this paper. By making integration tools easily accessible and facilitating the transition from prototype to real-world implementations, the framework seeks to lessen the cybersecurity load on app developers [41].

(ii) *Mobile Health and IoT Security: A Threat Modelling Approach:* This study highlights how crucial threat modeling is to comprehending the cybersecurity issues that IoT devices in mHealth systems pose. The method helps create more robust infrastructures to proactively reduce security vulnerabilities by methodically examining attack pathways and threats [42].

(iii) *Health Guard*: A Machine Learning-Based Security Framework for Smart Healthcare Systems. Health Guard is a security framework based on machine learning that was created to identify harmful activity in intelligent healthcare systems. Vital signs from linked devices are tracked, data is correlated to differentiate between benign and malicious activity, and various machine learning algorithms are employed to attain high detection accuracy [43].

These studies greatly improve cybersecurity in mHealth by offering practical frameworks and techniques for identifying and reducing possible risks.

4.1. Common Threats to mHealth Systems

(i) ***Data breaches:*** Unauthorized access to private health information is a common concern for mHealth systems, known as data breaches. To obtain personal health information, attackers may make use of flaws in communication networks, cloud storage, or mobile applications.

Smith claims that in addition to jeopardizing patient privacy, data breaches raise the possibility of financial fraud and identity theft. Adopting strong encryption procedures is necessary for healthcare providers to reduce the dangers of data breaches [44].

(ii) ***Man-in-the-Middle (MitM) Attacks:*** Threats involving MitM include cybercriminals intercepting device-to-healthcare system communications to steal or alter private information. These kinds of attacks can be especially harmful in mHealth applications that send real-time patient data to healthcare practitioners from wearable devices. [45] stress that in the absence of secure transmission mechanisms, hackers could obtain vital medical data, which could change treatment regimens and jeopardize patient safety.

(iii) ***Malware and ransomware:*** mHealth systems are at serious risk from ransomware and malware assaults, which infect devices and prevent access to patient data unless an amount of money is paid. Critical health information can be inaccessible due to these attacks, which can render mHealth apps or devices unusable. According to [46], because healthcare systems depend on instant access to patient data, fraudsters frequently target them, making healthcare organizations more susceptible to ransomware attacks. Such assaults may result in major financial losses and interruptions in patient treatment.

(iv) ***Device hijacking***: Remotely taking over mHealth devices by attackers is known as device hijacking, and it may result in system malfunctions or even patient injury. Inadequate security features make devices like remote diagnostic tools or wearable health monitors vulnerable to takeover. These attacks have the potential to cause delays in diagnosis, modify important patient data, and even manipulate medical treatments, all of which could directly jeopardize patient lives [47].

4.2. Emerging Threats

Attackers are increasingly focusing on healthcare systems and devices, according to recent patterns in cyberattacks, which present new security challenges for mHealth. For example, hackers are starting to take advantage of flaws in the Internet of Things (IoT)-connected devices that are used for medical diagnostics and patient monitoring. The risks of cyberattacks rise as healthcare systems embrace increasingly linked technology, such as AI-powered diagnostic tools [48]. The expanding application of AI in cyberattacks is a noteworthy emergent threat, as adversaries utilize AI algorithms to anticipate mHealth system vulnerabilities and automate the exploitation of those vulnerabilities [49]. Furthermore, attacks like Distributed Denial of Service (DDoS) attacks, which try to overwhelm healthcare infrastructure and make it inaccessible, have increased against hospital networks that deploy mHealth systems. Such attacks have the potential to seriously impair procedures, postpone medical interventions, and compromise patient safety [50-51]. The descriptions and solutions for securing embedded systems are presented in **Table 5**.

Table 5. Cybersecurity Threats, Mode of Attack, Challenges, and Solutions in Securing Embedded Systems.

Cybersecurity threat	Mode of attack/description	Challenges	Solutions	References
Ransomware Attacks	Attackers encrypt critical healthcare data, demanding payment for decryption. Medical devices may be rendered inoperable, affecting treatment.	Hospitals may face downtime, delays in treatment, or loss of access to patient records. These attacks threaten patient care continuity.	Regular backups of critical data Stronger access control and authentication Network segmentation to isolate sensitive systems	[46]
Data Breaches and Theft	Attackers gain unauthorized access to medical records, often through weak or stolen credentials. This data is sold on the black market or used for identity theft.	Stolen patient data can lead to identity theft, fraud, and privacy violations. The integrity and confidentiality of sensitive data are at risk.	Multi-factor authentication (MFA) Data encryption at rest and in transit Regular monitoring of access logs	[52]
Data Breaches	Illegal access to sensitive data in embedded systems	Protecting data at rest and in transit	Data encryption, access control mechanisms	[53]

Table 5. *Cont.*

Cybersecurity threat	Mode of attack/description	Challenges	Solutions	References
Denial of Service (DoS)	Attacks targeting the availability of embedded systems	Ensuring availability under malicious attacks	Intrusion detection systems, traffic filtering	[45]
Side-Channel Attacks	Attacks exploiting physical characteristics like power consumption or timing	Protecting against leakage of cryptographic keys	Countermeasures in hardware, noise injection	[51]
Malware	Malicious software designed to damage or disrupt embedded systems	Detection and removal of malware	Anti-malware systems, signature-based detection	[54]
Physical Attacks	Physical tampering with embedded devices	Securing hardware and preventing tampering	Tamper-proof designs, secure boot mechanisms	[16]

4.3. Comparing CTI-Driven Approaches with Traditional Security Models in mHealth

Traditional security paradigms are becoming less and less suitable as mHealth systems grow, depending on wearable technology, mobile platforms, and networked IoT infrastructure. Traditional methods like post-incident response plans, static firewalls, and antivirus software that rely on signatures mainly function reactively, dealing with threats only after they have already materialized [45]. In time-sensitive healthcare settings, where failure to identify and address cyber events promptly can have a direct impact on patient safety, this strategy is particularly troublesome.

The proactive paradigm offered by Cyber Threat Intelligence (CTI), on the other hand, uses predictive analytics and real-time threat data to foresee and reduce possible dangers. According to [55], CTI gathers and examines data from a variety of sources, such as threat feeds, adversary strategies, malware activity, and dark web activity, to make informed security decisions and anticipate attacks. By facilitating dynamic adaptation to new threats, CTI gives mHealth systems more resistance against sophisticated cyberthreats like ransomware and AI-driven attacks.

CTI is still not widely used in mHealth systems, despite its obvious benefits. The lack of defined threat formats, limitations on data sharing, and the resource limitations of mobile devices are among the issues that prevent widespread use [56]. But with more complex cyberattacks, it is becoming not only beneficial but also essential to incorporate CTI into mHealth cybersecurity frameworks.

5. Cyber Threat Intelligence for mHealth Data Security

5.1. Definition and Role of Cyber Threat Intelligence

Cyber Threat Intelligence (CTI) is the methodical gathering, analysis, and sharing of data about possible or existing cyber threats. CTI aims to help organizations comprehend, predict, and reduce cyber risks before they have a major impact [57] by looking at the tactics, techniques, and procedures (TTPs) that cyber criminals employ, CTI helps organizations take proactive steps to protect against threats by identifying patterns in cyberattacks, which aids in better defense and prediction strategies. Additionally, CTI enables organizations to improve their security posture, prioritize cybersecurity investments, and respond to things more efficiently [58].

5.2. CTI in Healthcare

CTI plays a crucial role in safeguarding mHealth (mobile health) data because the healthcare industry is becoming more and more susceptible to hackers. Due to the large volumes of sensitive data they store, particularly personal health information (PHI), healthcare institutions are often the focus of hackers. Healthcare professionals can utilize CTI to:

(i) ***Anticipate Vulnerabilities*****:** ***Anticipate Vulnerabilities*****:** Healthcare providers may keep up with the most recent attack methods and system weaknesses by utilizing

threat intelligence. They may give patching and system updates top priority thanks to this proactive approach [59]. CTI can assist in identifying typical attack patterns, particularly those that target mHealth devices such as wearables, mobile apps, and telemedicine platforms, by examining historical and current data regarding assaults on other healthcare institutions. For instance, [60] published in the Journal of Healthcare Security looked at the increasing frequency of ransomware attacks on healthcare facilities and showed how CTI technologies might identify potential targets by examining the changing strategies used by cybercriminal organizations.

(ii) ***Threat Detection:*** CTI helps healthcare businesses identify harmful behaviour in real time by enabling continuous monitoring of cybersecurity concerns. For instance, spotting odd traffic patterns or illegal access attempts may indicate an impending assault [61] CTI assists in threat detection by providing information about known attack signatures, strategies, and tactics that could be applied to mHealth systems. This involves keeping an eye out for indicators of compromise (IOCs) on social media, open-source intelligence, and dark web forums. [62] conducted research that created a CTI-driven strategy for mHealth systems that included predictive analytics with malware signature databases, enabling the early identification of cyberattacks before they became serious occurrences.

(iii) ***Prevention Strategies***: CTI facilitates the implementation of preventive measures by disseminating knowledge about known attack techniques. Healthcare businesses can use targeted defenses like firewalls, encryption, and multi-factor authentication to reduce the risk of cyberattacks by using knowledge of the behaviours of threat actors [63].

(iv) ***Incident Response Mechanisms:*** CTI offers helpful background information for handling cyber events. When a breach happens, CTI can assist in determining the type of assault, its possible consequences, and the most effective containment and recovery strategy. This makes it possible for medical institutions to react promptly and lessen the harm [64-65]. CTI contributes to improving incident response as well. CTI assists security teams in promptly determining the type of threat (such as ransomware, phishing, or data breach) when an attack is discovered, allowing for a more focused and efficient response. Recovery, forensic analysis, and quick confinement are all included in this.

5.3. Types of Threat Intelligence

Threat intelligence is divided into many levels according to the level of detail and breadth of the information presented. Every kind has a distinct function in assisting mHealth systems in anticipating, identifying, and addressing cyber threats.

(i) ***Strategic Intelligence***: This kind offers a broad perspective on the state of threats today. It contains information about new developing cyber threats, their possible effects, and more general trends in the cybersecurity space [66]. Decision-makers use strategic intelligence to develop long-term security plans. Strategic intelligence's function in mHealth is to comprehend which danger groups are aiming to harm healthcare facilities, what kinds of information they are looking for, and how healthcare systems are changing. Organizations can use this to change their long-term security plans from reactive to proactive. Example: State-sponsored threat actors are becoming a greater menace to the healthcare industry, according to Cisco's 2023 Global Threat Report. Healthcare firms should strengthen their defenses against these kinds of targeted assaults by learning about this trend through strategic CTI.

(ii) ***Tactical Intelligence***: Cybercriminals' tactics, motivations, and behaviors are the main focus of tactical intelligence. By understanding the tactics and tools used by threat actors, this kind of intelligence enables businesses to fight against particular attack types [67]. Organizations are better able to prepare for attacks when they are aware that a specific hacker gang employs phishing emails as a vector. Tactical intelligence plays a crucial role in mHealth systems by helping to predict the attack techniques that cybercriminals would employ to compromise devices, apps, or infrastructure. Preventive precautions can be implemented, for instance, if it is known that specific kinds of mobile malware frequently take advantage of out-of-date operating systems or inadequate authentication methods. [62] looked at how mHealth systems could strengthen their security posture by examining the methods that hackers employ to compromise mobile health apps. Their investigation revealed that phishing and inadequate app permissions were frequently used to take advantage of mHealth mobile app vulnerabilities.

(iii) ***Operational Intelligence:*** Operational intelligence focuses on particular attacks or situations. It contains comprehensive details about an ongoing cyberattack, including the attack's date, origin, and indicators of compromise (IOCs) [70]. This information is essential for containment and quick action. Operational intelligence is a vital source of information on recent attacks on health organizations. In-depth details about an ongoing cyberattack are included here, including the IP address of the perpetrator, the attack's tactics, and its extent. [68] detailed a CTI framework for mHealth that incorporated real-time data from healthcare institutions. Because of this operational information, a data breach in a wearable fitness monitoring app was quickly discovered, allowing for data recovery and prompt containment [47].

(iv) ***Technical Intelligence:*** This kind of intelligence is more detailed and covers technical topics, including attack vectors, vulnerabilities, and malware signatures. Organizations can implement precise technical defenses by comprehending particular attack methodologies, such as ransomware deployment methods or DDoS (Distributed Denial of Service) attacks [71]. The function of technical intelligence in mHealth systems is crucial in detecting particular vulnerabilities, like as malicious code or particular attack routes. This can entail spotting malware that targets medical equipment, flaws in data transfer methods, or vulnerabilities in the security of mobile apps. Recent research by [72] examined the increase in Bluetooth-based attacks directed at medical equipment in mHealth settings. Their study highlighted how crucial technical CTI is for locating particular attack vectors (such as Bluetooth vulnerabilities) and putting in place the necessary security solutions.

6. Integration of Cyber Threat Intelligence in Embedded Systems for Mhealth

Mobile health (mHealth) devices are becoming increasingly common in contemporary healthcare, and their security depends on embedded systems integrating Cyber Threat Intelligence (CTI). The adoption of CTI-driven security solutions is, however, fraught with difficulties because of interoperability problems, resource constraints, and the requirement for real-time processing. With an emphasis on the difficulties and possible solutions provided by CTI, this study explores the significance of incorporating CTI into embedded systems for mHealth. Additionally provided are case studies of effective CTI installations in the medical field.

6.1. Challenges in Integrating CTI with Embedded Systems

(i) ***Resource Limitations:*** Limited memory and processing power are characteristics of embedded systems. This presents a big problem when putting complicated CTI-based security solutions into practice, since they frequently call for a large investment of resources to process threat intelligence and carry out advanced analytics. CTI solutions are challenging to deploy in embedded systems with limited resources because they usually require huge data volumes and a lot of computing capacity. Lightweight security measures and improved algorithms are needed to overcome these obstacles and guarantee that the devices' functionality is unaffected [54].

(ii) ***Real-Time Processing Needs:*** mHealth devices work in real-time settings where patient safety depends on prompt threat identification and mitigation. There may be a mismatch between the computational capacity of embedded systems and the requirement for real-time processing. Furthermore, the addition of CTI-driven threat detection could result in latency, which would impair the device's overall functionality. To integrate real-time threat detection without interfering with the device's essential functions, effective anomaly detection models must be developed [73].

(iii) ***Interoperability***: mHealth systems frequently comprise a diverse range of platforms and devices, each with its own architecture and set of protocols. Interoperability issues arise when CTI-driven solutions are integrated into these heterogeneous environments. For CTI integration to be successful, smooth data interchange and communication between various systems must be ensured without sacrificing security. To solve interoperability problems, modular security frameworks and standardized protocols are crucial [74]

(iv) ***Complexity and Cost:*** High-security levels and related expenses or complexity are frequently traded off when integrating complex CTI-driven solutions into mHealth systems. Significant software and hardware in-

vestments are necessary to meet the demands of real-time analysis, improved threat identification, and ongoing monitoring. Scalable and flexible security solutions are becoming more and more necessary as the mHealth infrastructure grows in scale, which raises the deployment costs. When trying to procure a large number of devices within a budget, small healthcare providers may find these expenses onerous [52].

(v) ***User Compliance:*** Ensuring that patients and healthcare professionals adhere to security protocols is another major concern. Patients and healthcare professionals must follow established guidelines, such as regularly updating mobile devices, using strong passwords, and employing efficient encryption techniques, for CTI in mHealth to be effective, because wearable technology and mobile applications are so popular, it might be difficult to engage users and maintain consistent security procedures. Addressing behavioural challenges within mHealth security frameworks is essential since non-compliance could expose the system to cyberattacks [65].

6.2. Case Studies and Real-World Applications

To improve cybersecurity and safeguard private health information, CTI must be integrated with embedded systems in mHealth devices. The NHS and Apple HealthKit are two successful examples that demonstrate the significance of ongoing threat monitoring, real-time response systems, and cooperation between cybersecurity specialists and healthcare practitioners. Recent cyberattacks like ransomware and phishing campaigns have shown us the importance of proactive defenses, robust user authentication, and ongoing education. mHealth systems can greatly increase their resistance to cyberattacks by taking lessons from these examples and applying best practices.

6.2.1. Success Stories of Healthcare Systems Integrating CTI

Healthcare systems, especially mHealth devices, are using Cyber Threat Intelligence (CTI) more and more to improve data security and safeguard private patient data. The incorporation of CTI into the UK's National Health Service (NHS) is one noteworthy example of success. The NHS worked with several cybersecurity companies to put CTI tactics into place, which aid in identifying and reducing threats to healthcare data in real-time. Healthcare professionals use mobile health apps to access patient details, and the CTI system was integrated into the NHS's digital infrastructure. Proactive reactions to new threats and real-time notifications were made possible by this integration [75]. The Apple HealthKit platform is another effective example in the area of mHealth devices. Apple incorporates CTI into its ecosystem to safeguard data sent between healthcare systems and mobile devices. According to [47], the integration ensures compliance with health data privacy requirements like HIPAA and helps avoid assaults like illegal access to patient health data or data breaches.

6.2.2. Cyber Attack Case Studies

mHealth systems remain susceptible to cyberattacks despite CTI developments. The 2022 ransomware attack on a mHealth app used by a multinational healthcare organization made sensitive health information public. Through a technical flaw in the mobile app, the attackers could obtain encrypted health details without authorization. However, such threats may have been identified and eliminated before the attackers could encrypt the data if CTI systems had been put in place with real-time monitoring [68].

In 2023, a phishing effort attacked a mobile health care provider, resulting in another well-known cyberattack. Patient information and user credentials were lost as a result of the attackers' impersonation of the healthcare provider's customer service. Since CTI systems can recognize trends and send out alerts for questionable communications, this kind of social engineering attack might have been detected and stopped by integrating CTI into the system [69].

6.2.3. Successful CTI Implementation in Healthcare

An important illustration of CTI integration in healthcare is the application of anomaly detection systems in a network of wearables for managing chronic illnesses. The system effectively detected and prevented any attacks that could have compromised patient data without affect-

ing device function by integrating CTI. The solution offered strong protection by using threat intelligence feeds to detect behavioural anomalies in the devices and update malware signatures [69].

Furthermore, deploying CTI-driven security solutions in hospital networks to safeguard linked medical devices is another example. To prevent future data breaches and minimize downtime, the hospital was able to detect and respond to ransomware attacks by incorporating real-time threat intelligence into the network's embedded systems. By using CTI, the hospital was able to keep the system available and manage threats proactively [76].

6.3. Lessons Learned from Case Studies

a. These case studies have yielded several lessons that provide important information about combining CTI with embedded systems in mHealth. Active Threat Detection: It is essential to integrate CTI with embedded systems in real-time to continuously monitor risks. The benefits of ongoing monitoring, which can identify weaknesses and lower possible exposure, are demonstrated by the NHS and Apple HealthKit instances [77-78].

b. *Integration with Mobile Health Devices*: Embedded systems that can process and react to risks must be incorporated into the design of mHealth devices. Sensitive data can be protected from unwanted access by devices that use robust encryption and ongoing CTI. For example, if the app's security architecture had included more reliable embedded CTI systems, the 2022 ransomware assault might not have failed [79].

c. *User Education and Authentication*: Although CTI and embedded systems can offer great defences, it's also crucial to make sure users are informed about cyber threats and to use multi-factor authentication when using mobile health apps. Human error can still be a major weakness, as the 2023 phishing assault showed, necessitating integrated user education and awareness initiatives [80].

d. *Collaborative security efforts*: Building strong cybersecurity ecosystems for healthcare services requires public-private partnerships, such as those with the NHS. Real-time threat intelligence can be shared thanks to these initiatives, improving the healthcare system's overall security and protecting mHealth devices [81].

6.4. Cyber Threat Intelligence-Driven Security Solutions and Techniques for Enhancing Data Security in mHealth

Real-time health monitoring, data exchange, and communication between patients and healthcare professionals are made possible by mHealth applications, which make use of mobile devices and embedded systems. Significant worries about the privacy and security of sensitive health data accompany these advancements. With an emphasis on intrusion detection, secure firmware updates, access control, encryption, and authentication, this article explores the essential security features required for mHealth systems.

(i) Anomaly Detection Systems: The platforms and devices that make up mHealth systems are often diverse, each with its own architecture and set of protocols. The integration of CTI-driven solutions into these diverse environments gives rise to interoperability problems. The success of CTI integration depends on ensuring seamless data interchange and communication between different systems without compromising security. According to [82], Standardized protocols and modular security frameworks are essential for resolving interoperability issues.

(ii) Threat Signature Updates: Malware signatures should be updated often for embedded systems in order to help block known threats and stop vulnerabilities from being exploited. The system is kept safe from new threats thanks to the integration of CTI, which allows mHealth devices to get updated threat signatures regularly. This dynamic update technique ensures that embedded systems are always aware of the most recent information regarding cyber threats, which improves their security [83].

(iii) Contextual Awareness: The ability of CTI to provide contextual awareness enables embedded systems to identify particular risks that are pertinent to the healthcare setting. For instance, a security system that is controlled by CTI could differentiate between a bad actor trying to gain access to private information and a normal patient monitoring system. According to [84], CTI enhances the overall security of mHealth systems by allowing for more precise detection and response by taking into account the context in which a device functions.

(iv) Encryption Mechanisms: This includes light-

weight and data encryption in transit and at rest. *Lightweight Cryptography for Embedded Systems* mHealth devices usually have embedded systems with limited processing power, memory, and battery life. Thus, using effective cryptography methods is essential to safeguarding private information without compromising system functionality. The special requirements of embedded systems have led to the development of lightweight cryptographic algorithms like Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) [85]. Device data encryption is frequently done using AES, particularly its lighter forms, but ECC provides robust encryption with reduced key sizes, which makes it perfect for devices with constrained processing power [86]. Also*, data Encryption in Transit and at Rest:* Encryption must be used when data is being transmitted and stored on the device to guarantee patient data security. To prevent interception during transmission, data is frequently encrypted using Transport Layer Security (TLS) or its lightweight variant, Datagram TLS (DTLS) [87]. When patient data is at rest, it should be encrypted using strong algorithms like AES. Hardware security modules (HSMs) or trusted platform modules (TPMs) should be used to safely manage encryption keys [88].

(v) Authentication and Access Control: This includes MFA and RBAC. *Multi-Factor Authentication (MFA):* In mHealth systems, authentication procedures must guarantee that sensitive patient data is only accessible by authorized staff. Multi-factor authentication (MFA) greatly improves access control by combining many verification factors (something the user knows). One-time passwords (OTP), secure tokens, and biometric identification (facial recognition or fingerprint) are a few examples. According to [89], these safeguards are especially crucial for protecting access to mHealth devices, especially when handling sensitive medical data. Also, *Role-Based Access Control (RBAC):* In mHealth systems, role-based access control, or RBAC, is a crucial method for managing access. RBAC restricts access to resources by creating user roles (such as patient, healthcare professional, and administrator) according to the needs and role of the user. By limiting the possibility of unwanted access, this method guarantees that only the right people can access particular features or data. To guarantee that users are only given access to features and information pertinent to their jobs, RBAC is frequently incorporated into the operating system of embedded mHealth systems [90].

(vi) Secure Firmware and Software Updates: This includes OTA and secure boot, and trust anchors. *Over-the-Air (OTA) Updates:* Updates to firmware and software are necessary to guard against new vulnerabilities as embedded systems in mHealth devices grow more complicated. With over-the-air (OTA) updates, embedded systems may be updated securely from a distance, keeping devices safe without the need for human intervention. To guard against malicious code injection and unauthorized tampering, OTA updates ought to be encrypted and authenticated [53]. Also, *Secure Boot and Trust Anchors:* Safe boot procedures guarantee that only approved, unaltered firmware can start a device. Because devices in mHealth systems may be susceptible to malicious attacks or physical tampering, this is especially crucial. The firmware integrity is checked before the device wakes up with the use of trust anchors, which are frequently implemented using hardware-based security measures like Trusted Platform Modules (TPMs) [91]. Because only genuine and secure firmware is installed, thanks to these security measures, hackers are unable to compromise the device during the boot-up phase.

(vii) Intrusion Detection and Prevention Systems (IDPS): For embedded mHealth systems to be monitored in real-time and to identify and react to questionable activity, intrusion detection and prevention systems, or IDPS, are necessary. IDPS can detect new attack patterns and offer proactive threat detection by integrating Cyber Threat Intelligence (CTI). These systems keep an eye on device logs, network traffic, and system behaviours to spot possible security lapses and stop them before they do any harm [92].

The techniques, descriptions, strengths, and weaknesses for enhancing data security in mHealth using embedded systems are presented in **Table 6**.

Table 6. Techniques, Description, Strengths, and Weaknesses for Enhancing Data Security in mHealth Using Embedded Systems.

Techniques	Description	Strengths	Weaknesses	References
Encryption	The process of converting data into a format that is unreadable without the correct decryption key.	Ensures data confidentiality. Prevents unauthorized access.	Computationally expensive. Can impact performance on embedded devices.	[85]
Access Control	Mechanisms to restrict access to data and resources based on user roles or authentication credentials.	Limits unauthorized access. Enhances data privacy.	Requires complex configuration. Potential for misconfigurations.	[66]
Secure Boot	A method that ensures a device starts only with trusted software, preventing unauthorized code execution.	Protects against malware and firmware attacks. Increases device trust.	Implementation can be complex. May introduce delays during booting.	[53]
Intrusion Detection Systems (IDS)	A system that monitors network or system activities for malicious actions or policy violations.	Real-time threat detection. Can detect novel attack patterns.	Can generate false positives. Resource intensive for embedded systems.	[21]
Biometric Authentication	Using unique biological characteristics (fingerprint, facial recognition, etc.) to verify identity.	High level of security. Difficult for attackers to bypass.	Requires specialized hardware. Privacy concerns around biometric data.	[89]
Hardware-Based Security (TPM)	Trusted Platform Modules (TPM) are used to provide secure storage of cryptographic keys and sensitive data.	Provides tamper-resistant storage. Enhances trust in hardware.	Hardware dependencies. Increased device cost and complexity.	[51]
Blockchain for mHealth	Using decentralized ledgers to secure and verify health data transactions, ensuring immutability.	Provides immutable data records. Enhances data integrity.	Can be slow in processing large datasets. Energy consumption can be high.	[98]
Machine Learning for Anomaly Detection	Using machine learning algorithms to detect anomalies in device behavior, signaling potential security threats.	Can detect unknown threats. Adaptive to new attack techniques.	Requires large datasets for training. High resource consumption.	[54], [93]

7. Future Directions in Applying CTI in mHealth

Technologies for mobile health (mHealth) are quickly transforming the medical field by facilitating real-time data processing, ongoing monitoring, and individualized treatment. The correct operation of mHealth systems depends on security and privacy, which are major issues raised by these developments. It is becoming more widely acknowledged that improving the security of mHealth technology requires the use of Cyber Threat Intelligence (CTI). This study examines the difficulties in integrating CTI into mHealth systems and talks about new developments that can improve the security architecture of mHealth solutions in the future.

(i) AI and Machine Learning: Machine learning (ML) and artificial intelligence (AI) have the potential to significantly improve CTI for mHealth, and enhance it [94]. According to [95] AI and ML models can predict vulnerabilities based on past data, automate threat detection, and

evaluate vast amounts of health data to find odd trends. By learning from new threats and adjusting to new dangers without human intervention, these technologies can also facilitate ongoing security measure improvement and identify anomalous patterns before they develop into more serious risks. AI-powered predictive analytics may help avert possible security breaches.

(ii) Blockchain for Data Integrity: Blockchain technology is becoming more and more popular as a potent instrument to improve mHealth systems' data security and integrity. Because mHealth data is decentralized (for example, gathered from several sensors, wearables, and devices), it is essential to guarantee the immutability and authenticity of health information. Only authorized users can view and alter health data stored on the blockchain's distributed ledger system, which provides a transparent and safe method of doing so [96],[98]. Additionally, by enabling patients and healthcare professionals to trace the history of data updates, blockchain's audit trail feature can increase confidence in mHealth systems.

(iii) Post-Quantum Cryptography: There is a lot of uncertainty around the future of cryptography systems due to the emergence of quantum computing. Current cryptographic systems that protect mHealth data could be broken by quantum computers, thus, it's critical to be ready for the difficulties presented by these threats. Creating new cryptographic algorithms that can withstand attacks by quantum computers is known as post-quantum cryptography (PQC) [97]. mHealth providers need to start using these new algorithms, even though PQC is still in its infancy, to future-proof their security architecture and guarantee that private health information is safeguarded as quantum computing becomes more widely available.

8. Conclusions

The critical role embedded systems play in enabling remote patient monitoring, data collection, and real-time health treatments in mobile health (mHealth) applications is highlighted in this paper. The growing dependence on these systems, however, also poses serious cybersecurity threats. To strengthen data security in mHealth, the review emphasizes the significance of Cyber Threat Intelligence (CTI). To facilitate preventive security measures and incident response, CTI can offer insightful information about new threats, vulnerabilities, and attack patterns. The review's conclusion emphasizes the necessity of ongoing study and teamwork among embedded systems developers, cybersecurity specialists, and healthcare practitioners. In the quickly changing mHealth landscape, this cooperation is crucial to predicting and reducing evolving cyber threats and protecting the confidentiality of critical patient data. The mHealth landscape relies heavily on embedded systems for data collection and transmission, making robust cybersecurity crucial. Cyber Threat Intelligence (CTI) plays a vital role in real-time threat detection and mitigation, but its integration with embedded systems requires careful consideration of resource limitations and interoperability. Future advancements in mHealth security will depend on emerging technologies like blockchain, post-quantum cryptography, AI, and ML. To stay ahead of evolving cyber threats, continuous collaboration between healthcare, cybersecurity, and embedded system experts is essential. This partnership should focus on developing innovative CTI-driven solutions, leveraging cutting-edge technologies to enhance data security, and establishing uniform security policies. Ultimately, these efforts will safeguard patient data and facilitate the growth of mHealth technology.

Author Contributions

For research articles with several authors, a short paragraph specifying their individual contributions must be provided. The following statements should be used "Conceptualization, ACI and VCU; methodology, VCU and ACI; formal analysis, ACI.; resources, VCU; writing—original draft preparation, ACI.; writing—review and editing, URA.; visualization, VCI.; supervision, URA.; project administration, URA . All authors have read and agreed to the published version of the manuscript." Authorship must be limited to those who have contributed substantially to the work reported.

Funding

There is no external funding received by the authors.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

No datasets were generated or analysed during the current study.

Acknowledgments

We sincerely acknowledge the Management of Veritas University Abuja and Alex Ekwueme Federal University Ndufu-Alike, for granting us the enabling environment to thrive. Also, to all whose works are cited both in print and electronically. Finally, we greatly appreciate our interested readers for finding this paper useful. Thank you.

Conflicts of Interest

The authors declared that there is no conflict of interest in this article. The Authors utilized AI tools such as Grammarly for grammatical checks.

References

[1] Anikwe, C.V., Nweke, H.F., Ikegwu, A.C., et al., 2022. Mobile and wearable sensors for data-driven health monitoring system: State-of-the-art and future prospect. Expert Systems with Applications. 202, 117362. DOI: https://doi.org/10.1016/j.eswa.2022.117362

[2] Dinh-Le, C., Chuang, R., Chokshi, S., et al., 2019. Wearable health technology and electronic health record integration: scoping review and future directions. JMIR mHealth and uHealth. 7(9), e12861. DOI: https://doi.org/10.2196/12861

[3] Chakraborty, C., Bhattacharya, M., Pal, S., et al., 2024. From machine learning to deep learning: Advances of the recent data-driven paradigm shift in medicine and healthcare. Current Research in Biotechnology. 7, 100164. DOI: https://doi.org/10.1016/j.crbiot.2023.100164

[4] Ksira, Z., Mellit, A., Blasuttigh, N., et al., 2024. A novel embedded system for real-time fault diagnosis of photovoltaic modules. IEEE Journal of Photovoltaics. 14(2), 354–362. DOI: https://doi.org/10.1109/JPHOTOV.2024.3359462

[5] Ikegwu, A.C., Nweke, H.F., Anikwe, C.V., et al., 2022. Big Data Analytics for Data-driven Industry: A Review of Data Sources, Tools, Challenges, Solutions and Research Directions. Cluster Computing. 25(5), 3343–3387. DOI: https://doi.org/https://doi.org/10.1007/s10586-022-03568-5

[6] Mahler, T., Nissim, N., Shalom, E., et al., 2018. Know your enemy: Characteristics of cyber-attacks on medical imaging devices. Available from: https://arxiv.org/abs/1801.05583 (cited 1 January 2025).

[7] Ewoh, P., Vartiainen, T., 2024. Vulnerability to cyberattacks and sociotechnical solutions for health care systems: systematic review. Journal of medical internet research. 26, e46904. DOI: https://doi.org/10.2196/46904

[8] Xing, Y., Lu, H., Zhao, L., et al., 2024. Privacy and security issues in mobile medical information systems MMIS. Mobile Networks and Applications. 29, 762–773. DOI: https://doi.org/10.1007/s11036-024-02299-8

[9] Ameen, A.H., Mohammed, M., Rashid, A., 2023. Dimensions of artificial intelligence techniques, blockchain, and cyber security in the Internet of medical things: Opportunities, challenges, and future directions. Journal of Intelligent Systems. 32(1), 20220267. DOI: https://doi.org/10.1515/jisys-2022-0267

[10] Abdulhussein, M., 2024. The impact of artificial intelligence and machine learning on organizations cybersecurity [PhD Thesis]. Lynchburg, VA: Liberty University. pp. 1-273.

[11] Willie, M.M., 2023. The role of organizational culture in cybersecurity: building a security-first culture. Journal of Research, Innovation and Technologies. 2(2(4)), 179–198. DOI: https://doi.org/10.57017/jorit.v2.2(4).05

[12] Ahmadi, H., Arji, G., Shahmoradi, L., et al. 2019. The application of internet of things in healthcare: a systematic literature review and classification. Universal Access in the Information Society. 18, 837–869. DOI: https://doi.org/10.1007/s10209-018-0618-4

[13] Wang, M., Ji, H., Jia, M., et al., 2023. Method and application of information sharing throughout the emergency rescue process based on 5G and AR wearable devices. Scientific Reports. 13(1), 6353. DOI: https://doi.org/10.1038/s41598-023-33610-4

[14] Istepanian, R.S., Woodward, B., 2016. M-health: Fundamentals and Applications. John Wiley & Sons: Hoboken, NJ, USA. pp. 1-85.

[15] Nweke, H., Ikegwu, A.C., Nwafor, C.A., et al., 2024. Smartphone-based human activity recognition using Artificial Intelligence Methods and Orientation Invariant Features. Nigeria Computer Society. 35, 1–8.

[16] Singh, B., Kaunert, C., 2024. Unmanned aerial vehicle: Integration in healthcare sector for transforming interplay among smart cities. In: Khan, I.U., Hajjami, S.E., Ouaissa, M., Belaqziz, S., Bhatia, T.K. (eds.).

Cognitive Machine Intelligence. CRC Press: Boca Raton, FL, USA. pp. 108–129.
[17] Suppiah, R., Noori, K., Abidi, K., et al., 2024. Real-time edge computing design for physiological signal analysis and classification. Biomedical Physics & Engineering Express. 10(4), 045034. DOI: https://doi.org/10.1088/2057-1976/ad4f8d
[18] Parmar, R., Patel, D., Panchal, N., et al., 2022. 5G-enabled deep learning-based framework for healthcare mining: State of the art and challenges. Blockchain Applications for Healthcare Informatics. 401–420. DOI: https://doi.org/10.1016/B978-0-323-90615-9.00016-5
[19] Sharmila, V., Kannadhasan, S., Rajiv Kannan, A., et al., 2024. Challenges in Information, Communication and Computing Technology. Proceedings of the 2nd International Conference on Challenges in Information, Communication, and Computing Technology (ICCICCT 2024); April 26–April 27, 2024; Namakkal, India. pp. 1–890.
[20] Nolte, H., 2024. Utilizing HPC Systems to Serve Compute-Intensive Tasks from a Data Lake Managing Sensitive Data [PhD Thesis]. Göttingen: Georg-August-Universität Göttingen. pp. 1–173.
[21] Kumar, A., Singh, A.K., Choi, B.J., 2021. Analysis of User Interaction to Mental Health Application Using Topic Modeling Approach. In: Kim, J.H., Singh, M., Khan, J., Tiwary, U.S., Sur, M., Singh, D. (eds.). International Conference on Intelligent Human Computer Interaction, Lecture Notes in Computer Science, vol 13184. Springer: Cham, Switzerland. pp. 703–717.
[22] Choi, J.R., 2022. Exploring the surveillance culture in the context of smart health: a cross-cultural comparison between South Korea and the US [PhD Thesis]. Austin, TX: The University of Texas at Austin. pp. 1-231.
[23] Zhang, H., Ibrahim, A., Parsia, B., et al., 2023. Passive social sensing with smartphones: a systematic review. Computing. 105(1), 29–51. DOI: https://doi.org/10.1007/s00607-022-01112-2
[24] Huang, C., Wang, J., Wang, S.H., et al., 2023. Internet of medical things: A systematic review. Neurocomputing. 557, 126719. DOI: https://doi.org/10.1016/j.neucom.2023.126719
[25] El-Amrawy, F., Nounou, M.I., 2015. Are Currently Available Wearable Devices for Activity Tracking and Heart Rate Monitoring Accurate, Precise, and Medically Beneficial? Healthcare Informatics Research. 21(4), 315–320. DOI: https://doi.org/10.4258/hir.2015.21.4.315
[26] West, D.M., 2013. Improving health care through mobile medical devices and sensors. Brookings Institution Policy Report. 10(9), 1–13.
[27] Rajendran, S., Porwal, A., Anjali, K., et al., 2024. Portable IoT Devices in Healthcare for Health Monitoring and Diagnostics. In: Murthy, H., Zurek-Mortka, M., Pillai, V.J., Kumar, K.P. (eds.). Internet of Things in Bioelectronics: Emerging Technologies and Applications. Wiley: Hoboken, NJ, USA. pp. 263–296.
[28] Salama, R., Altrjman, C., Al-Turjman, F., 2024. Healthcare cybersecurity challenges: a look at current and future trends. Computational intelligence and Blockchain in complex systems. 97–111. DOI: https://doi.org/10.1016/B978-0-443-13268-1.00003-0
[29] Nisha, S., 2025. Securing Life-Saving Devices: Challenges and Solutions in Medical Device Cybersecurity. International Journal of Trend in Scientific Research and Development. 9(1), 776–783.
[30] Balaji, V., Sonowal, G., Gowda, S., 2024. Recent Research Techniques in Processing, Security, and Storage of Real-World Applications of Big Computing. In: Sardar, T.H., Pandey, B.K. (eds.). Big Data Computing. CRC Press: Boca Raton, FL, USA. pp. 145–179.
[31] Gonzalez, I., Calderón, A.J., Folgado, F.J., 2022. IoT real time system for monitoring lithium-ion battery long-term operation in microgrids. Journal of Energy Storage. 51, 104596. DOI: https://doi.org/10.1016/j.est.2022.104596
[32] Kramer, D.B., Yeh, R.W., 2017. Practical improvements for medical device evaluation. JAMA. 318(4), 332–334. DOI: https://doi.org/10.1001/jama.2017.8976
[33] Sonko, S., Monebi, A.M., Etukudoh, E.A., et al., 2024. Reviewing the impact of embedded systems in medical devices in the USA. International Medical Science Research Journal. 4(2), 158–169. DOI: https://doi.org/10.51594/imsrj.v4i2.767
[34] Yun, J., Rustamov, F., Kim, J., et al., 2022. Fuzzing of embedded systems: A survey. ACM Computing Surveys. 55(7), 1–33. DOI: https://doi.org/10.1145/3538644
[35] Khan, S., Jiangbin, Z., Ullah, F., et al., 2024. Hybrid computing framework security in dynamic offloading for IoT-enabled smart home system. PeerJ Computer Science. 10, e2211. DOI: https://doi.org/10.7717/peerj-cs.2211
[36] Garg, A., Kumar, A., Singh, A.K., 2024. Machine Learning-Based Security Approaches for Wireless Body Area Networks. In: Singh, A.K., Kumar, S. (eds.). Security, Privacy, and Trust in WBANs and E-Healthcare. CRC Press: Boca Raton, FL, USA. pp. 206–235.
[37] Nahta, P., 2025. Securing the Digital Supply Chain: Challenges, Innovations, and Best Practices in Cybersecurity. In: Lytras, M.D., Alkhaldi, A., Serban, A.C. (eds.). Innovation Management for a Resilient Digital Economy. IGI Global Scientific Publishing:

Hershey, PA, USA. pp. 205–230.

[38] Aslam, M.M., Tufail, A., Apong, R.A.A.H.M., et al., 2024. Scrutinizing security in industrial control systems: An architectural vulnerabilities and communication network perspective. IEEE Access. 12, 67537–67573. DOI: https://doi.org/10.1109/ACCESS.2024.3394848

[39] Kumar, A., Kumar, A., Tomar, G.S., et al., 2023. Advanced Wireless Communication: Technology Overview, Challenges, and Security Issues. In: Bagwari, A., Tomar, G.S., Bagwari, J., Victória Barbosa, J.L., Sastry, M.K.S. (eds.). Advanced Wireless Communication and Sensor Networks. Chapman and Hall/CRC: New York, NY, USA. pp. 65–80

[40] Gowda, D., Reddy, P., Rajasekhara, V., et al., 2025. Revolutionizing Patient Care Through the Convergence of IoMT and Generative AI. In: Kumar, V.V., Katina, P.F., Zhao, J.Y. (eds.). Convergence of Internet of Medical Things (IoMT) and Generative AI. IGI Global Scientific Publishing: Hershey, PA, USA. pp. 217–242.

[41] Thantilage, R.D., Yasarathna, T.L., Le-Khac, N.-A., et al., 2023. Secure Emergency Data Sharing in Healthcare-A Data Warehouse View. Available from: https://www.researchsquare.com/article/rs-3659636/v1 (cited 1 January 2025).

[42] Sahu, A.K., 2024. Multimedia watermarking: Latest developments and trends. Springer Nature: Berlin, Germany. pp. 1–136.

[43] Chen, C.-S., Chen, W.-C., 2019. Research on a remote monitoring system for automatic control on dairy farms. In: Lam, A.K.T., Prior, S., Shen, S.-T., Young, S.-J., Ji, L.-W. (eds.). Engineering Innovation and Design. CRC Press: London, UK. pp. 285–290.

[44] Abbasi, N., Smith, D.A., 2024. Cybersecurity in Healthcare: Securing Patient Health Information (PHI), HIPPA compliance framework and the responsibilities of healthcare providers. Journal of Knowledge Learning and Science Technology. 3(3), 278–287. DOI: https://doi.org/10.60087/jklst.vol3.n3.p.278-287

[45] Singh, N., Buyya, R., Kim, H., 2025. Securing Cloud-Based Internet of Things: Challenges and Mitigations. Sensors. 25(1), 1–45. DOI: https://doi.org/10.3390/s25010079

[46] Jones, L.A., Burrell, D.N., 2025. Illegal Cybersecurity Threats Created by Organizational Arsonists in Healthcare Organizations. Law, Economics and Society. 1(1), 93. DOI: https://doi.org/10.30560/les.v1n1p93

[47] Kumar, R., 2024. Privacy and protection of patient sensitive data in the healthcare sector: a critical analysis [M.Sc.]. Dehradun: UPES. pp. 1-101.

[48] Wang, P., Jiang, C., Mao, A. W., Sun, Q., Zhu, H., Inman, J., ... & Chang, H. (2024). An AI-Powered tissue-agnostic cellular morphometrics biomarker for risk assessment in patients with pan-gastrointestinal precancerous lesions and cancers. *medRxiv*, 2024-11.

[49] Zhang, Z., Ning, H., Shi, F., et al., 2022. Artificial intelligence in cyber security: research advances, challenges, and opportunities. Artificial Intelligence Review. 55, 1029–1053. DOI: https://doi.org/10.1007/s10462-021-09976-0

[50] Nguyen, D.C., Pham, Q.-V., Pathirana, P.N., et al., 2022. Federated learning for smart healthcare: A survey. ACM Computing Surveys (Csur). 55(3), 1–37. DOI: https://doi.org/10.1145/3501296

[51] Ozcelik, M.M., Kok, I., Ozdemir, S., 2025. A Survey on Internet of Medical Things (IoMT): Enabling Technologies, Security and Explainability Issues, Challenges, and Future Directions. Expert Systems. 42(5), e70010. DOI: https://doi.org/10.1111/exsy.70010

[52] Tan-Smith, C., 2023. Medicalised Ketogenic Therapy Practice [PhD Thesis]. Te Pūkenga: Otago Polytechnic. pp. 1–405.

[53] Zhang, L.C., 2020. Interworking Mechanism of Blockchain Platforms for Secure Tourism Service [Master's Thesis]. Jeju City: Judo National University. pp. 1–95.

[54] Xu, H., Seng, K.P., Ang, L.M., et al., 2024. Decentralized and distributed learning for AIoT: A comprehensive review, emerging challenges and opportunities. IEEE Access. 12, 101016–101052. DOI: https://doi.org/10.1109/ACCESS.2024.3422211

[55] Basheer, R., Alkhatib, B., 2021. Threats from the Dark: A Review over Dark Web Investigation Research for Cyber Threat Intelligence. Journal of Computer Networks and Communications. 2021(1), 302999. DOI: https://doi.org/10.1155/2021/1302999

[56] Zhou, M., Ruan, S., Liu, J., et al., 2022. vtpm-sm: An application scheme of SM2/SM3/SM4 algorithms based on trusted computing in cloud environment. Proceedings of 2022 IEEE 15th International Conference on Cloud Computing (CLOUD); July 10–July 16, 2022; Barcelona, Spain. pp. 351–356.

[57] Abohatem, A.Y., Ba-Alwi, F.M.M., Al-Khulaidi, A.A.G., 2023. Suggestion cybersecurity framework (CSF) for reducing cyber-attacks on information systems. Sana'a University Journal of Applied Sciences and Technology. 1(3), 234–252. DOI: https://doi.org/10.59628/jast.vli3.248

[58] Prince, N.U., Mamun, M.A.A., Olajide, A.O., et al., 2024. IEEE standards and deep learning techniques for securing internet of things (iot) devices against cyber-attacks. Journal of Computational Analysis and Applications. 33(7), 1270–1289.

[59] Tahmasebi, M., 2024. Beyond defense: Proactive approaches to disaster recovery and threat intelligence in modern enterprises. Journal of Information Secu-

rity. 15(2), 106–133.
[60] Van W. A., 2024. Legislation within cybersecurity: preparing for NIS2–a detailed framework in the healthcare sector in the Netherlands [Master's Thesis]. Turku: University of Turku. pp. 1–158.
[61] Ejjami, R., 2024. Enhancing Cybersecurity through Artificial Intelligence: Techniques, Applications, and Future Perspectives. Journal of Next-Generation Research 5.0. 1(1). DOI: https://doi.org/10.70792/jngr5.0.v1i1.5
[62] Singh, P., Singh, N., Singh, K.K., et al., 2021. Diagnosing of disease using machine learning. In: Singh, K.K., Singh, A., Elhoseny, M., Elngar, A.A. (eds.). Machine learning and the internet of medical things in healthcare. Elsevier: Amsterdam, The Netherlands. pp. 89–111.
[63] Fontem, O., 2024. Strategies and Methods Used by Information Technology Security Professionals to Secure Cloud Access Infrastructure [PhD Thesis]. Minneapolis, MI: Walden University. pp. 1–158.
[64] Mehrotra, A., Zampetakis, M., Kassianik, P., et al., 2024. Tree of attacks: Jailbreaking black-box llms automatically. Advances in Neural Information Processing Systems. 37, 61065–61105.
[65] Miller, M.D., Redfern, R.E., Anderson, M.B., et al., 2024. Completion of patient-reported outcome measures improved with use of a mobile application in arthroplasty patients: results from a randomized controlled trial. The Journal of Arthroplasty. 39(7), 1656–1662. DOI: https://doi.org/10.1016/j.arth.2024.01.007
[66] Cinar, B., 2023. A Study on Cyber Threat Intelligence Based on Current Trends and Future Perspectives. In: Rafatullah, M., Santoso, L.W. (eds.). Advances and Challenges in Science and Technology Vol. 5. BP International: Kolkata, India. p. 37.
[67] Verma, O.P., Verma, S., Perumal, T., 2024. Advancement of intelligent computational methods and technologies. CRC Press: Boca Raton, FL, USA. pp. 1–206.
[68] Popoola, O.J., 2025. Designing a Privacy-Aware Framework for Ethical Disclosure of Sensitive Data [PhD Thesis]. Sheffield: Sheffield Hallam University. pp. 1–374.
[69] Li, N., Xu, M., Li, Q., et al., 2023. A review of security issues and solutions for precision health in Internet-of-Medical-Things systems. Security and Safety. 2, 2022010. DOI: https://doi.org/10.1051/sands/2022010
[70] Aminu, M., Akinsanya, A., Oyedokun, O., et al., 2024. Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. International Journal of Computer Applications Technology and Research. 13(8), 11–27. DOI: https://doi.org/10.7753/IJCATR1308.1002
[71] El-Amir, S., 2023. Comprehensive Cybersecurity Review: Modern Threats and Innovative Defense Approaches. International Journal of Computers and Informatics (Zagazig University). 1, 30–37.
[72] Hang, C.-N., Tsai, Y.-Z., Yu, P.-D., et al., 2023. Privacy-enhancing digital contact tracing with machine learning for pandemic response: a comprehensive review. Big Data and Cognitive Computing. 7(2), 108. DOI: https://doi.org/10.3390/bdcc7020108
[73] Zhang, C., Yang, S., Mao, L., et al., 2024. Anomaly detection and defense techniques in federated learning: a comprehensive review. Artificial Intelligence Review. 57(6), 150. DOI: https://doi.org/10.1007/s10462-024-10796-1
[74] Ndlovu, K., Mars, M., Scott, R.E., 2021. Interoperability frameworks linking mHealth applications to electronic record systems. BMC health services research. 21(1), 459. DOI: https://doi.org/10.1186/s12913-021-06473-6
[75] Ofoegbu, K.D.O., Osundare, O.S., Ike, C.S., et al., 2024. Enhancing cybersecurity resilience through real-time data analytics and user empowerment strategies. Engineering Science & Technology Journal. 4(6), 689–706. DOI: https://doi.org/10.51594/estj.v4i6.1527
[76] Chen, B., Shi, X., Feng, T., et al., 2024. Construction and Application of a Private 5G Standalone Medical Network in a Smart Health Environment: Exploratory Practice From China. Journal of medical internet research. 26, e52404. DOI: https://doi.org/10.2196/52404
[77] Volpe, U., Elkholy, H., Gargot, T., et al., 2023. Devices, Mobile Health, and Digital Phenotyping. In: Tasman, A., Riba, M.B., Alarcón, R.D., Alfonso, C.A., Kanba, S., Lecic-Tosevski, D., Ndetei, D.M., Ng, C.H., Schulze, T.G. (eds.). Tasman's Psychiatry. Springer: Cham, Switzerland. pp. 5191–5216.
[78] Young, S., 2024. The Science and Technology of Growing Young, Updated Edition: An Insider's Guide to the Breakthroughs that Will Dramatically Extend Our Lifespan... and What You Can Do Right Now. BenBella Books: Dallas, TX, USA. pp. 1–288.
]79] Jansen, E., Supplieth, J., Lech, S., et al., 2025. Process evaluation of technologically assisted senior care using mixed methods: Results of the virtual assisted living (VAL, German: VBW Virtuell Betreutes Wohnen) project. Digital health. 11, 20552076241308445. DOI: https://doi.org/10.1177/20552076241308445
[80] Leong, C., 2024. An Exploratory Sequential Mixed Methods Study On Usable Cybersecurity And The Behaviorial Effects Of Cognitive Load [PhD Thesis]. Orlando, FL: University of Central Florida. pp. 1–88.
[81] Nag, A., Hassan, M.M., Das, A., et al., 2024. Exploring the applications and security threats of Internet of

Thing in the cloud computing paradigm: A comprehensive study on the cloud of things. Transactions on Emerging Telecommunications Technologies. 35(4), e4897. DOI: https://doi.org/10.1002/ett.4897

[82] Im, H., Lee, D., Lee, S., 2024. A novel architecture for an intrusion detection system utilizing cross-check filters for in-vehicle networks. Sensors. 24(9), 2807. DOI: https://doi.org/10.3390/s24092807

[83] Patnala, V.N., Dinakarrao, S.M.P., Venkataramani, G., et al., 2024. Special Session: Detecting and Defending Vulnerabilities in Heterogeneous and Monolithic Systems: Current Strategies and Future Directions. Proceedings of 2024 International Conference on Compilers, Architecture, and Synthesis for Embedded Systems (CASES); September 29–October 4, 2024; Raleigh, NC, USA. pp. 5–14.

[84] González-Pérez, A., Matey-Sanz, M., Granell, C., et al., 2023. AwarNS: A framework for developing context-aware reactive mobile applications for health and mental health. Journal of Biomedical Informatics. 141, 104359. DOI: https://doi.org/10.1016/j.jbi.2023.104359

[85] Zhou, X., Li, B., Qi, Y., et al., 2020. Mimic encryption box for network multimedia data security. Security and Communication Networks. 2020(1), 8868672. DOI: https://doi.org/10.1155/2020/8868672

[86] Poh, G.S., Gope, P., Ning, J., 2019. PrivHome: Privacy-preserving authenticated communication in smart home environment. IEEE Transactions on Dependable and Secure Computing. 18(3), 1095–1107. DOI: https://doi.org/10.1109/TDSC.2019.2914911

[87] Alenezi, M.N., Al-Anzi, F.S., 2021. A study of Z-transform based encryption algorithm. International Journal of Communication Networks and Information Security. 13(2), 302–309. DOI: https://doi.org/10.17762/ijcnis.v13i2.5052

[88] Zhou, X., Guan, J., Xing, L., et al., 2022. Perils and Mitigation of Security Risks of Cooperation in Mobile-as-a-Gateway IoT. Proceedings of the ACM Conference on Computer and Communications Security; November 7–November 11, 2022; Los Angeles, CA, USA. pp. 3285–3299.

[89] Gao, S., Wang, Q., Liu, Y., et al., 2021. A Privacy-Preservation Scheme based on Mobile Terminals in Internet Medical. Available from: https://www.researchsquare.com/article/rs-288792/v1 (cited 5 January 2025).

[90] Batista, E., Moncusi, M.A., López-Aguilar, P., et al., 2021. Sensors for context-aware smart healthcare: A security perspective. Sensors. 21(20), 6886. DOI: https://doi.org/10.3390/s21206886

[91] Tawffaq, M.R., et al. 2024. IoT Security in a Connected World: Analyzing Threats, Vulnerabilities, and Mitigation Strategies. Proceedings of 2024 36th Conference of Open Innovations Association (FRUCT); October 30–November 1, 2024; Lappeenranta, Finland. pp. 626–638.

[92] Jain, R., Rai, M.S.S., 2023. Energy-Efficient and Secure Routing Protocol for Wireless Sensor Networks. Energy. 8(2).

[93] Ikegwu, A.C., Obianuju, O.J., Nwokoro, I.S., et al., 2025. Investigating the Impact of AI/ML for Monitoring and Optimizing Energy Usage in Smart Home. Artificial Intelligence Evolution. 6(1), 30–43. DOI: https://doi.org/https://doi.org/10.37256/aie.6120256065

[94] Mathew, D.E., Ebem, D.U., Ikegwu, A.C., et al., 2025. Recent Emerging Techniques in Explainable Artificial Intelligence to Enhance the Interpretable and Understanding of AI Models for Human. Neural Processing Letters. 57, 16. DOI: https://doi.org/10.1007/s11063-025-11732-2

[95] Abbas, H., Ansari, N.M., Sattar, A., et al., 2025. Enhancing Cryptographic Security with Deep Learning: Intelligent Threat Detection and Attack Prevention. Spectrum of engineering sciences. 3(2), 195–225.

[96] Kumar, R., Kumar, P., C.C., S., et al., 2025. Blockchain and AI in Shaping the Modern Education System. CRC Press: Boca Raton, FL, USA. pp. 1–284.

[97] Song, B., Kim, T., 2024. Analyzing Recent Research Trends in Post-Quantum Cryptography Using Latent Dirichlet Allocation. Proceedings of 2024 15th International Conference on Information and Communication Technology Convergence (ICTC); October 6–October 18, 2024; Jeju Island, Korea. pp. 92-97. IEEE

[98] Li, X., Cheng, J., Shi, Z., et al., 2023. Blockchain security threats and collaborative defense: A literature review. Computers, Materials and Continua. 76(3), 2597–2629. DOI: https://doi.org/10.32604/cmc.2023.040596