Discover Computing

REVIEW Open Access

Cyber threats in mobile healthcare applications: systematic review of enabling technologies, threat models, detection approaches, and future directions

Anayo Chukwu Ikegwu[1,2*], Uzoma Rita Alo[1] and Henry Friday Nweke[3,4]

*Correspondence:
Anayo Chukwu Ikegwu
ikegwua@veritas.edu.ng
[1]Computer Science Department, Faculty of Physical Sciences, Alex Ekwueme Federal University Ndufu-Alike, P.M.B 1010, Abakaliki, Ebonyi State, Nigeria
[2]Software Engineering Department, Faculty of Natural and Applied Sciences, Veritas University Abuja, Abuja, Nigeria
[3]Computer Science Department, David Umahi Federal University of Health Sciences, P.M.B 211, Uburu, Ebonyi State, Nigeria
[4]International Institute for Machine Learning, Robotics and Artificial Intelligence Research, David Umahi Federal University of Health Sciences, P.M.B 211, Uburu, Ebonyi State, Nigeria

Abstract

Mobile healthcare (mHealth) delivery has revolutionized the healthcare industry 5.0. With the move toward mHealth, access to healthcare services has gradually increased, allowing individualized treatment routines, and real-time health monitoring. However, cybersecurity threats to mHealth systems also increase as their use increases. The continuous rise of cyber threats has recently affected the healthcare delivery sector. These have caused much financial damage and fears in the past few years. This paper aims to systematically assess and categorize the cyber threats in mHealth applications to guide the industry-wide adoption and prospects. A systematic literature review was carried out between 2018 and 2025 including 40 primary study papers were synthesized out of 24,854 search articles. The study discussed mHealth, trends, features, and main technologies to explore the advancement of mHealth. It presents cyber threats in mHealth applications where the common cyber threats were identified and security challenges such as data compromise, malicious attacks, insecure systems, and user vulnerabilities. We provided mitigation strategies to address the inherent challenges. It further highlights traditional and contemporary and centralized and decentralized detection approaches to cyber threats for effective implementation of patient health data. The findings showed that much work is left undone which we offered in open research prospects. The outlined open research prospects will improve the security and privacy of health-sensitive data against cyber threats. The practical implication of this study is that it will guide all health stakeholders, such as patients, health professionals, agencies, government and policymakers, and researchers, in improving the security and privacy of patients' data in digital cyberspace.

Keywords Cyber threat, Cybersecurity, Mobile healthcare applications, MHealth, Review, Threat intelligence

1 Introduction

Mobile healthcare (mHealth) is defined as "mobile computing, medical sensor, and communication technologies for healthcare" [1, 2]. According to the Harvard Business Review (HBR), mHealth and telehealth were not widely used until the advent of smartphones and the development of more sophisticated revolution per minute (RPM) technology allowed for a more interactive form of healthcare [2]. During the pandemic, telehealth accounted for 69% of all doctor-patient visits. Telehealth is distinct from telemedicine in that it encompasses a wider range of remote medical services. Telehealth also refers to non-clinical services like provider training, continuing medical education or public health education, administrative meetings, and electronic information sharing to support and facilitate assessment, diagnosis, consultation, treatment, education, and care management, even though telemedicine refers specifically to remote clinical services [2]. mHealth delivery has become a revolutionary guide that involves the delivery of healthcare services, remote monitoring, and management of health-related issues such as mental health, cardiovascular disease, and dementia [3]. It is now possible for patients and healthcare providers to use assistive wearable sensors, mobile devices, and health-tracking apps [4]. With the move toward mobile healthcare, access to healthcare services has gradually increased, allowing individualized treatment routines, and real-time health monitoring. However, cybersecurity threats mHealth systems have increased as their use increases. Cyber threats, including ransomware attacks, data breaches, hacking incidents, unauthorized access, theft, improper disposal, etc., find mobile healthcare applications appealing because they can gather and handle extremely sensitive patient data [5, 6]. Safeguarding this information against online attacks is essential for upholding patient confidentiality and guaranteeing the accuracy and accessibility of medical services.

The continuous rise of cybersecurity threats activities has speedily affected the healthcare sector recently. These have caused much financial damage and fears in the past few years. Some hospitals and healthcare providers have recently incurred financial losses due to cyber threats. For example, CommonSpirit Health incurred over $150 million, Scripps Health (over $11 8,700,000), Change Healthcare ($872,000,000), etc. from legal fees, remediation, and data breach mitigation [7, 8]. With an average of 1,463 cyberattacks per week in 2022, up 74% from 2021, and an average cost of $1 million for each breach, the healthcare sector is the largest and fastest-growing industry to face multi-million-dollar fines [7]. In addition, over 10 healthcare providers experienced disruption to patient care which cost an average of $1.47 million to restore normal healthcare services [9]. It was highlighted in IBM's 2024 report, that an average of $9.77 million per incident is incurred by healthcare organisations that are associated with data breaches between the years 2023 and 2024 marking it the biggest cyber-attack [10, 11]. Sensitive data drives this since it often relies on legacy systems. Medical records contain some sensitive information such as date of birth, social security number (SSN), bank verification number (BVN), national identification numbers (NIN), etc. are normally vulnerable and valuable to threat actors or hackers for identity theft and fraudulent practices. According to a recent survey, Joel [12] examined hospitals with a bed count of one thousand or more that were shut down for an average of more than 6 h, at an hourly rate of $21,500. At a staggering cost of $47,500 per hour, the shutdowns frequently lasted more than 9 h for smaller hospitals.

Mobile healthcare could be best explained as a practice of medical and public health underpinned by a technological framework that makes use of mobile and Internet of Things (IoT) devices to improve data generation, communication, collaboration, and health-related tasks [13]. mHealth plays a crucial role in modern healthcare. It enhances access to healthcare, particularly in underserved and remote areas, by enabling remote diagnostics, virtual consultations, and real-time monitoring of patients' health conditions. It helps patients track their fitness and wellness, manage chronic conditions more effectively, and receive timely interventions, all while easing the strain on healthcare infrastructure. It further accelerates data collection and analysis easier for better decision-making and personalized care, making healthcare more efficient, affordable, and accessible. The enormous contribution of mHealth makes it attractive to cyber threats.

A cyber threat could mean any malevolent attempt or action meant to interfere with, harm, or obtain unauthorized access to computer networks, systems, or data [5, 14]. This is aimed at compromising confidentiality, integrity, or availability of information. Cyber threats can appear in different forms, such as ransomware, phishing, malware, hacking, and denial-of-service (DoS) assaults [15]. Often referred to as hackers or state-sponsored actors, these threats normally emanate from people, groups, or organisations that calculatedly tend to steal confidential data, interfere with business operations, or take advantage of system flaws for financial, political, or private benefit [16]. Moreover, the systematic methods and tools used to identify malicious activity, illegal access, or possible weaknesses in digital systems such as networks and wearable devices, software applications, etc., are referred to as cyber threat detection [17, 18]. As cyberattacks have become more sophisticated, detection methods have changed to incorporate artificial intelligence, machine learning, and advanced analytics such as federated learning, which allows for the quicker discovery of patterns and abnormalities that may point to danger. By emphasizing early detection using federated learning to stop harm, these solutions enable businesses and investors to proactively guard against malware, data breaches, and other online and physical threats.

Currently, there are peculiar security challenges that affect the rapid adoption, implementation, and deployment of mHealth services as highlighted by some studies. For example, Sullivan [19] noted that incidences of ransomware attacks have decreased, but it is still a constant threat to healthcare institutions. A healthcare professional may inadvertently click on a malicious link, giving hackers access to vital systems [20]. Traditional DoS attacks only employ one source [21]. Still, Distributed Denial of Service (DDoS) attacks [14, 15] use numerous systems to increase the attack's impact, making prevention more difficult. The cyber threats hinder patient treatment, system security, and dependability. The unidentified attackers obtain important data about the security token of the Rivest-Shamir-Adleman (RSA) algorithm—an authentication method that creates one-time keys to improve online security—by using secure APIs [22]. Consequently, the major security challenges include data compromise, malicious attacks, insecure systems, and user vulnerabilities [20, 23–26].

1.1 Related studies

Recently, quite a few research studies have explored cyber threats in mobile healthcare applications. Some of these studies have reviewed cyber threats, detection, mobile security, and mobile health systems for health monitoring. For instance, an earlier study by

Weichbroth et al. [27] presented a survey on mobile security, highlighting the threats and best operational practices. However, the study concentrated only on mobile security and failed to discuss its applicability to mobile health, nor did it consider cybersecurity threats. Sakib [28] carried out cyber threat assessments, vulnerability, cycle of intelligence, guidelines formulation, and recommendations. Nonetheless, this study focuses on cyber threats in general and is not tailored to mobile healthcare applications. A related survey by Arazzi et al. [29] highlighted natural language processing techniques, challenges, and potential impacts from a cybersecurity threat intelligence perspective. Nevertheless, mobile health applications were not targeted. Alenoghena et al. [30] presented an extensive survey on mHealth architecture, development, security, and mitigation. However, the study focused on electronic health (eHealth) practices, and cyber threats is not addressed in the study. A recent review by Cartwright [31],

Furthermore, Aldhaheri [32] presented a review of cyber threat detection based on deep learning techniques in Internet of Things (IoT) networks. The study discussed complex cybersecurity advancements and challenges, such as intrusion detection systems (IDS) in IoT. Nonetheless, the review focused on only IDS applications in IoT and never discussed IDS in mHealth. Also, Mahboubi [33] explored a systematic review of cyber threat hunting using evolving techniques. The study discussed hypothesis formulation, threat-hunting methods, and challenges. However, the study doesn't cover mobile healthcare applications. A more recent study by ElSayed et al. [34] explored a comprehensive survey on the cyber-attacks, impact, and strategies to address on Internet of Things (IoT) in healthcare systems. However, the study focuses on cyberattacks on IoT in healthcare systems and does not specifically discuss cyber threats in mobile healthcare systems.

Conversely, the current study differs from the existing related studies. First, the systematic review focused on mobile health, discussing trends, features, main technologies' strengths, and weaknesses. Second, we discussed cyber threat approaches for mobile healthcare applications, discussing the strengths and weaknesses of each threat in the context of mHealth settings. Finally, we extensively highlighted the security challenges and mitigation strategies peculiar to mHealth. Consequent upon this, this systematic review is a well-construed assessment of current cyber threats in mHealth applications, challenges, mitigation strategies or solutions, and future research prospects of mobile health adoption, developments, and deployments. Based on our knowledge from the extensive studies reviewed, there are no comprehensive systematic reviews or surveys that enshrine all-encompassing cyber threat-based mobile health themes.

Consequently, this paper aims to systematically assess and categorize the current cyber threats in mobile healthcare applications to guide the industry-wide adoption and future prospects.

The significant contributions of this paper to the current body of knowledge are as follows:

- We provided an in-depth discussion of mobile health, trends, features, main technologies,
- We extensively discussed cyber threats in mHealth including traditional and contemporary approaches, weaknesses, and strengths in cyber threat detection;
- We further provided centralized and decentralized detection approaches in cyber threat detection;

- Also, we presented an analysis of the growing adoption of mHealth applications and security challenges;
- Provides strengths and weaknesses of common cyber threats to mHealth;
- More so, we provided mitigation strategies to address the growing security challenges;
- Additionally, we explored future research directions in implementing cyber threat detection in mHealth environments.

Other sections of the paper are broken down as follows: Sect. 2 explores the methodology, Sect. 3 discusses the mobile healthcare system, Sect. 3.1 highlights the evolution of mHealth, and the main technologies enabling mobile healthcare are presented in Sect. 3.2. Also, Sect. 4 delves into the cyber threats in mobile healthcare applications, while Sect. 4.1 discusses the growing adoption of mobile healthcare applications and security challenges while the mitigation strategies for cyber threats in the mHealth setting are covered in Sect. 4.2. Cyber threat detection approaches to mHealth applications are discussed in Sect. 5. Then, Sect. 5.1 presents traditional and contemporary approaches whereas centralized and decentralized approaches are discussed in Sect. 5.2. Furthermore, a discussion of the study is presented in Sect. 6. Open research direction is handled in 8.

The layout of the paper is depicted in Fig. 1.

2 Methodology

This section discusses the approaches by which the research study materials or articles were obtained. The systematic review study was adopted and reported according to the guidelines proposed by Carrera-Rivera et al. and Randles & Finnegan [35, 36] for computer science and engineering disciplines. Following the procedural guidelines, several methods were discussed, including research questions, search strategy, inclusion and exclusion criteria, screening process, data extraction, and quality assessment.

2.1 Research questions

The research questions set the pace for the systematic review process as outlined.

RQ1: How has the evolution of mobile healthcare systems impacted the delivery of personalized healthcare services over the past decade?

RQ2: What are the main technologies driving the growth of mobile healthcare systems, and how do they enable improved patient care and monitoring?

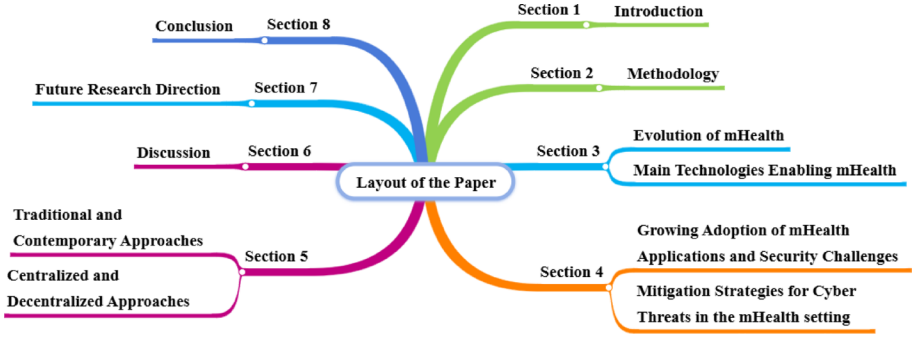

Fig. 1 The Layout of the Paper

RQ3: How does the growing adoption of mobile healthcare applications impact the security challenges associated with their use?

RQ4: What mitigation strategies have been proposed or implemented to address cyber threats in mobile healthcare applications?

RQ5: What are the cyber threats that are most prevalent in mobile healthcare applications, and what vulnerabilities do they exploit?

RQ6: Which future research direction is the researcher's concentration on cyber threats in mHealth applications?

2.2 Search strategy

The literature search was conducted for a wide coverage of primary studies on cyber threats in mHealth apps. This study was carried out through an electronic search from 9 major academic databases such as Google Scholar, PubMed, ACM Digital Library, SpringerLink, Web of Science, MedLine, IEEE Xplore, DOAJ, and ScienceDirect for articles published between the years 2018 and 2025 The initial search was performed using keyword combinations such as "cyber threats" AND/OR "mobile" AND "healthcare" AND/OR "applications", "cyber" AND "security" AND "attack" to identify papers published between the specified years (2018–2025) in all 9 academic databases. The abstract was utilized to extract the relevant information and avoid bias in selection. Secondly, another search was conducted using a combination of keywords, such as "cybersecurity threats" AND "mobile" AND "healthcare" AND "applications" to identify articles published between 2018 and 2025 in Web of Science, Google Scholar, PubMed, ACM Digital Library, ScienceDirect, SpringerLink, and IEEE Xplore. This second search was conducted because cyber and/or cybersecurity threats are often used interchangeably when relating to mHealth.

2.3 Inclusion and exclusion criteria

This systematic study focuses on applying cyber threats in mHealth settings instead of the wider eHealth settings. It examines how cyber threats can be used with threats or breaches identified by mobile devices to solve real-world healthcare issues. Intrinsically, articles that detected new cybersecurity threats but were not precisely considered for mobile healthcare applications were excluded. In addition, only articles published in adjudicated journals and conference proceedings were examined. Moreover, other kinds of publications were excluded, including books of abstracts, books, conference abstracts only, commentaries, and editorials. Also, excluded are articles not written in English, not peer-reviewed and/or not presented at reputable conferences, publication year earlier than 2018, and lack relevance to the subject of discourse. Furthermore, publications written in English languages and publications dated from 2018 to 2025 were included.

2.4 Screening process

Using a database search, 24,854 publications were found, and 13,080 studies and 173 duplicate studies were eliminated using each database's content-type filter. After screening the titles and abstracts, 11,536 of the 11,601 remaining articles were eliminated, leaving only 65 pertinent articles. After a last round of screening, 40 out of the 65 papers were determined to be eligible for inclusion and were added to the review, and 25 papers were discarded due to inconsistency and non-alignment. Using the inclusion

and exclusion criteria mentioned above, two authors independently reviewed the titles and abstracts of the identified articles to decide which ones qualified for this systematic review. The reviewers came to a consensus after exchanging minor points of contention. The study selection screening process is shown in Fig. 2.

2.5 Data extraction

Out of the 24,854 articles searched, only 40 were finally selected for further analysis. These 40 publications were classified into the following 4 categories: cyber threat types, vulnerabilities, impact, and solutions strategies within mobile healthcare applications. The included articles were divided into these four auspicious areas.

2.6 Quality assessment

A critical stage in systematic reviews and meta-analyses is assessing the quality of the papers included in the study to ensure the findings are grounded in consistent evidence.

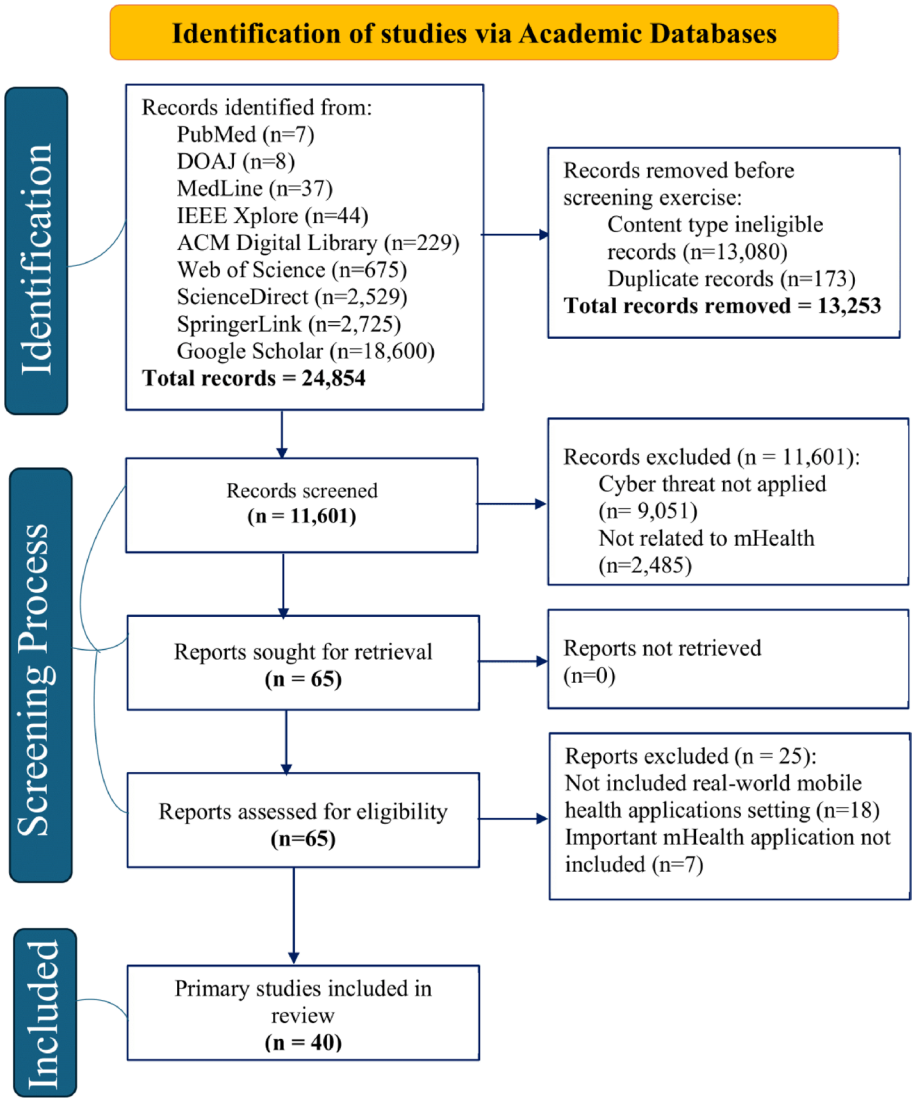

Fig. 2 The study selection screening process

When choosing papers, deciding whether the topic is relevant is paramount. These might trigger some questions.

(i) Are the proposed research topic and solutions important to the research?
(ii) Does the research paper demonstrate a comprehensive cyber threat and its detection?
(iii) Does the research paper state its objective very well?
(iv) Does the research compare various cyber threat approaches?

3 Mobile healthcare systems

The mobile healthcare system plays a crucial role in modern healthcare. The term "mobile healthcare (mHealth) system" refers to the entire infrastructure or system that facilitates the use of mobile technologies for medical and health purposes [1]. The use of mobile technologies for medical purposes is known as mobile healthcare [37]. The basic pillars of mHealth include communication systems, medical sensors, and computer/mobile computing. It has apps that decrease emergency room (ER) visits, enhance health outcomes, and promote communication between patients and the healthcare system. It improves access to healthcare, particularly in underserved and remote areas, by enabling remote diagnostics, virtual consultations, and real-time monitoring of patients' health conditions. It helps patients track their fitness and wellness, manage chronic conditions more effectively, and receive timely interventions, all while easing the strain on healthcare infrastructure. It further accelerates data collection and analysis for better decision-making and personalized care, making healthcare more efficient, affordable, and accessible.

3.1 The evolution of mobile health

Basic communication tools have given way to sophisticated, AI-enabled platforms that facilitate real-time monitoring, diagnosis, and individualized treatment in mobile healthcare spaces. Mobile technology, wearables, and connection advancements are driving this trend, which could improve patient-centred, patient-accessible, and efficient healthcare [1, 38, 39]. Telemedicine began as early as the 1960 s when the National Aeronautics and Space Administration (NASA) pioneered remote medical monitoring for astronauts during space missions, which sparked a study into remote healthcare systems by the military [1, 38]. The U.S. military experimented with remote medical support in remote areas for about the same period. Additionally, the first telemedicine consultations were conducted remotely using simple audio and video hook-ups, enabling doctors to diagnose and counsel patients in remote rural areas. The advent of mobile telephony increased in the 1990 s, and the use of cell phones for healthcare services, including the exchange of text messages between patients and doctors, became evident [1].

In the early 2000 s, the use of smartphones, particularly Apple's iPhone in 2007, mobile healthcare underwent a drastic change, opening the door for the creation of applications that may provide interaction and real-time health monitoring [6, 40]. Additionally, mHealth apps were developed for tracking fitness, reminding people to take their medications, and disseminating health information. Calorie counting, exercise tracking, and basic health metrics monitoring were done with simple apps. Early remote diagnostic devices, such as glucometers and ECG monitors, were made possible by Bluetooth and other wireless technologies like HeadTrack [41], mesh aggregation techniques [42], live migration approach [43], which allowed data to be sent straight to medical healthcare

providers [40]. The growth of wearables, IoT, and mobile-based telemedicine expanded tremendously in the 2010s [39, 44, 45]. Wearables such as the Fitbit, Apple Watch, and other fitness trackers that provided real-time data on steps, heart rate, sleep, and ECG readings were quickly adopted. Through integration with Internet of Things (IoT) advancements, these wearables and mobile devices were able to link to a wider ecosystem of health monitoring technologies, giving healthcare providers access to real-time data. With the expansion of mobile-based telemedicine platforms, patients can now consult with doctors through mobile applications [46]. Secure messaging, real-time data sharing, and video calls have become essential components of remote care.

Furthermore, the trend of mobile healthcare systems has become increasingly a reality. The deployment and adoption of mobile-based healthcare services made it easy for every household and healthcare provider to interact with them daily. For instance, from the 2020s to date, artificial intelligence (AI) enhanced mHealth and remote monitoring of patients caused a trajectory of immense contribution [38, 47]. Artificial intelligence [48] is now used by mobile health apps to provide personalized health advice, predictive analytics, and diagnostic support. AI-powered chatbots offer basic triage, symptom checking, and round-the-clock support. Remote patient monitoring (RPM) [13], which uses wearable and mobile technology to track patients' health data (such as blood pressure and glucose levels) and notify healthcare providers of any changes, proved crucial during and after the coronavirus (COVID-19) pandemic. To maintain healthcare accessibility and reduce in-person visits, pandemic responses like COVID-19 spurred the development of mobile healthcare through contact tracing apps, symptom checks, and virtual care solutions. Additionally, the advancement of mobile-based applications continued to revolutionize the healthcare sector with emerging technologies and future directions [26, 49]. These technologies include advanced biometric sensors, 5G and beyond, blockchain for safe data interchange, predictive health analytics (such as machine learning, deep learning, etc.), federated learning for safe data privacy and security [50], etc. The mobile health trends, features, and descriptions are presented in Table 1.

3.2 Main technologies enabling mobile healthcare

The key or main technologies deployed for mobile healthcare include but are not limited to wireless communication, the Internet of Things (IoT) and Internet of Medical Things (IoMT), data analytics and AI, and cloud computing. These technologies are discussed in the subsection.

3.2.1 Wireless communication technologies for mobile healthcare

Wireless communication devices have brazened up for effective mobile health delivery. It is a digital device that aids and enhances file sharing and end-to-end data transfer. Wireless communication technologies make effective and distant healthcare delivery possible, allowing health data to be transmitted between equipment, patients, and healthcare practitioners. The key benefits include enhanced accessibility, improved efficiency, cost-effectiveness, and real-time monitoring essential to mHealth [4, 52, 53]. Some wireless communication technologies widely utilized for mHealth include Bluetooth, Wi-fi, cellular networks such as 4G and 5G, and Zigbee and Z-Wave [54, 55]. For instance [55], saw the importance of cellular network (internet access) for surpassing other targeted variables with an average of 83.41% in realizing the United States government's Healthy

Table 1 Trends, features, and descriptions of mobile health

Trends	Features	Descriptions	Author
Early Telemedicine Experiments (1960–1980 s)	NASA, military innovations, and early video consultations	Space mission begins research with remote healthcare technologies before combined telemedicine for remote patient consultations via an access link with video, audio, etc.	[1, 38]
Growth of Mobile Telephony (1990s)	Cell phone emergence and text-based health campaigns	Advancement of mobile phone technology for healthcare providers, non-profit, and public health sectors experimented with short message service (SMS) to disseminate public health-related information.	[1, 38]
Rise of Smartphones and Mobile Health Apps (2000s)	Smartphone introduction, first mHealth apps, and remote diagnostics	Smartphones were launched e.g. Apple's iPhone, which saw the creation of mobile apps integrated with wireless devices such as Bluetooth, and remote diagnostics tools such as electrocardiography (ECG) monitors, etc. that help with data transmission across healthcare providers.	[6, 40]
Wearable Health Technology and Integration with IoT (2010s)	Integration with IoT and mobile-based telemedicine platforms	Increase in wearable usage such as Fitbit, Apple smartwatches, fitness trackers, etc., and integration of IoT. Also, the rapid expansion of telemedicine via video calls, real-time data sharing, and coordination between patients and physicians.	[39, 44, 45]
AI-Enhanced Mobile Health and Remote Patient Monitoring (2020s-Present)	AI in mobile health, RPM, and pandemic response	Describe the collaboration of mobile health applications with the advent of AI to patient health monitoring to ensure healthcare accessibility and reduce in-person visits.	[13, 47, 48]
Emerging Technologies and Future Directions	5G and beyond, advanced biometric sensors and predictive health analytics (e.g. machine learning, deep learning, etc.), blockchain for secure data exchange, federated learning for secure data privacy and security	The increase of 5G global adoption and incorporation of wearable complex sensors for early signs detection and secure patient data management using [51] blockchain technology approach	[23, 34, 48]

People 2020 (HP2020) health is objectively achieved as a basis, which Healthy People 2030 (HP2030) will facilitate. Also, Bluetooth technology was effectively utilized for COVID-19 contact tracing to receive signals for proximity detection [54]. In addition, modern wireless body sensors have created a potential market for wearable technology that allows remote healthcare monitoring, free physical examination particularly for the elderly; creative biomedical signal recording devices are being used in hospitals and home healthcare services to assist physicians in their decision-making [56, 57].

3.2.2 IoT, IoMT in mobile healthcare

The Internet of Things (IoT) and the Internet of Medical Things (IoMT) have contributed to the real-time tracking of patients' health parameters/metrics [58]. The two ground-breaking technologies (IoT and IoMT) brought innovations in mobile healthcare [59, 60]. More effective and individualised care is made possible by these systems (IoT and IoMT), which are based on networked sensors and devices that gather, send, and evaluate health data in real-time. The Internet of Things is a network of linked items and gadgets that communicate online to share information [61]. Applications such as smart hospital equipment, wearable health monitoring, and remote care solutions are made possible by IoT in the healthcare industry [62]. The Internet of Medical Things is a subset of the Internet of Things that is specifically focused on the healthcare industry [60,

63]. It includes wearable technology, medical devices, and software that support health management, diagnosis, and treatment. IoMT provides a smooth flow of medical data by integrating with clinical systems. Severally studies have utilised these technological devices or equipment for the implementation of healthcare delivery systems. For example, an earlier study by Haoyu et al. [64] implemented IoMT cloud-based enabled sensors such as blood oxygen (SpO_2) and heart rate variability for the detection of sleep apnea in real-time. Additionally, a recent study by Zhang et al. [65] utilised wireless IoMT channels to enable model training on long-tail data connected to work together with several mobile clients and one edge server (ES). This helps the model to achieve an increased average accuracy from 4.44 to 28.36%. However, investigating communication resource allocation techniques that allow clients to successfully upload their local models to take part in the aggregate, even if they have more tailored data and poor transmission conditions, remains open. Furthermore, Aminifar et al. [66] deployed IoT equipment to secure a privacy-preserving edge federated learning over mobile health and wearable devices. The proposed framework was achieved through Amazon's AWS cloud, based on real-world IoT requests. Nonetheless, further study is required on the implementation of Byzantine, Poisoning, and Backdoor attacks in mobile healthcare data.

3.2.3 Data analytics and artificial intelligence in mobile healthcare

The data analytics and AI application is centred on how to improve decision support, tailored medicine, and diagnostics in mobile healthcare. By facilitating intelligent data processing, predictive insights, and individualised care, data analytics and artificial intelligence are revolutionizing mobile healthcare [67]. By enabling patients, researchers, and healthcare professionals to make well-informed decisions, these tools enhance effectiveness and health outcomes. To produce relevant insights, data analytics such as descriptive, predictive, and prescriptive analytics processes vast amounts of health data from multiple sources, including wearable technology, mobile apps, and electronic health records [68, 69]. Data analytics and AI techniques further enhance decision-making, and proactive care, and provide scalable solutions, personalised experiences, and cost reduction. Numerous authors have utilised data analytics and AI models to deliver effective healthcare solutions to users. For instance, Vekaria et al. [70] utilised data analytics with an AI model (e.g. Long-Short Term Memory) to predict COVID-19 and boost the economy. It makes smart cities lucrative and healthy by controlling pandemics and boosting the economy in the process. However, additional AI models are required for generality testing. Other recent works that discuss the application of data analytics and artificial intelligence models/algorithms for mHealth implementation for health monitoring and privacy preservation include [3, 71–73]A more recent study by Khamaj [74] utilized an AI chatbot interface using machine learning and natural language processing to improve the timely appointments of elderly patients, which makes it more sensitive. Nonetheless, the effectiveness of these AI-based solutions in comparison to their long-term use and assessment of the extent to which the population's quality of life has improved can be given more attention. Engaging technology developers and healthcare practitioners, however, will aid in expanding the use and application of these technologies to specific user groups.

3.2.4 Cloud computing in mobile healthcare

Cloud computing (CC) is transforming mobile healthcare by offering creative, economical, and adaptable ways to manage and provide medical services. Scaling, integrating various data sources, and supporting cutting-edge technologies like artificial intelligence guarantee its pivotal place in the future of digital healthcare [75, 76]. The CC is important for developing mobile health applications and monitoring. It offers excellent benefits such as remote accessibility, scalable infrastructure, data storage and management, as well as advanced analytics and AI [77]. Different works have deployed cloud computing methods to improve mobile healthcare development. For instance, an early study by Kumar et al. [78] secured storage and its accessibility via cloud-based to diagnose and predict disease using a fuzzy neural model. Cloud computing system offers business models through data insight [79].

The main technologies, descriptions, weaknesses, strengths, and application areas for mobile healthcare are presented in Table 2.

4 Cyber threats in mobile healthcare applications

In recent times, cybersecurity practice has grown, especially the shared concerns activities of some stage actors such as hackers, nation-states, hacktivists, Yahoo Boys (Internet fraudsters), G^{++} (advanced level of fraudulent schemes), Scammers, and Cybercriminals. Cybersecurity is the systematic approach to securing systems, theft, networks, illegal access, and data from digital attacks or threats [25, 81]. It includes all necessary strategies, tools, and practices devised to mitigate against unauthorized users, breaches, and cyber threats. The increase in the use of digital and network devices in our daily activities has led to the rise of security concerns. One of the variable factors of cybersecurity is the cyber threat environment, which has become a threat landscape that triggers the

Table 2 Main technologies enabling mobile healthcare, descriptions, challenges, strengths and application areas

Technologies	Description	Weakness	Strength	Applications	Author
Wireless Communication Technologies	Allow health data to be transmitted between devices, patients, and practitioners	Data privacy and security, high initial costs, network reliability, interoperability	Cost savings, enhanced accessibility, improved efficiency, real-time monitoring, and patient-centric care	RPM, telemedicine and virtual consultations, smart healthcare facilities, mobile health apps, emergency response	[54–56]
IoT and IoMT	A network of integrating devices that communicate online to share information	Data privacy and security, implementation cost	Real-time data exchange and personalized healthcare	RPM, telemedicine integration, medication adherence solutions, emergency response systems	[59, 60, 65, 66, 80]
Data Analytics and AI	Improve decision support, tailored medicine, and diagnostics in mobile healthcare	Data privacy, security, bias in AI models, interoperability, Regulatory compliance, and patient adoption	Enabling intelligent data processing, predictive insights, and personalized care.	Personalized medicine, remote diagnostics, virtual health assistants, and disease prediction and early detection	[3, 68, 72]
Cloud Computing	providing scalable and accessible infrastructure for managing, storing, and analyzing health data	Data privacy and security, internet dependency, regulatory compliance, and interoperability issues	Cost efficiency, enhanced accessibility, scalability, security and compliance, and improved collaboration	Collaborative research, health administration, RPM, telemedicine services, mobile apps	[75, 76, 78]

different stage actors to employ sophisticated methods to exploit vulnerabilities for disruption and financial benefits. Other key elements of cybersecurity include information privacy, software privacy, networking privacy, and node authenticity [25]. Cyber threats are viewed as any harmful practice that intentionally seeks to steal important data or cause damage to system resources [82]. Besides, cyber threats have caused a lot of havoc to humanity and system networks, weakening the Internet of Things (IoT), Internet of Everything (IoE), and Internet of Medical Things (IoMT) based infrastructural resources [31, 46, 65], and dynamic network function virtualization [83]. Cyber threat detection is the practice of monitoring and examining system activity, data, and network traffic to spot possible security risks like viruses, flaws, or illegal access attempts [84, 85]. It entails utilizing a range of analytics methods, such as machine learning and artificial intelligence, to identify, stop, and mitigate assaults instantly.

Detecting cyber threats in data, flaws, state actors, and unusual due to activities is important to ensure maximum safety and proactive cybersecurity defence in our organizations [86]. Several studies have explored cybersecurity measures, tools, and analytics methods such as AI/ML, federated learning, deep learning, etc., to tackle cyber threats. For example, Duary et al. [25] explored the use of AI and collaborative approaches in detecting cyber threats while maintaining ethical concerns. However, more collaborative efforts among the developers, researchers, and implementation of advanced methods/tools are needed. Labu & Ahammed [81] leverage AI and machine learning methods to detect fraudulent activities in the Feedzai security system using a transaction record dataset. The result shows that the random forest (RF) machine learning detected cyberattacks with an accuracy of 79.23%. However, the study requires improvements by enabling real-time cyber-threats fraud detection using Feedzai's app and advanced machine learning techniques. Dey et al. [82] implemented a metaheuristic-based AdaBoost and RF feature selection framework to detect cyber threats in IoT networks using 49 features that have its placed as target features with about 25,40,044 sample sizes. The result obtained shows that RF performs better due to the optimised feature subset of 4 out of 42 features. Also, RF with 99.41% accuracy and an F1-score of 99.33%, and the lowest false positive rate of 3%. Nonetheless, the framework needs an enhancement to address zero-day cyber threats generated from IoT network traffic. A study by Ai [20] highlighted trends and the future for utilising ML techniques for the detection of cyber threats. The author revealed that the practical and real-life implementation of anomaly detection, feature extraction, and classification approaches is highly needed for cyber threat detection. The study also pointed out some peculiar challenges requiring attention, such as data quality and quantity issues, model interpretability and transparency, and adversarial attacks on analytic models.

Security and privacy are vital in overcoming cyber threats [86, 87]. When the network infrastructure and its application resources are secured, it proactively addresses some inherent problems associated with cyber threats, such as hacker vulnerability exploitation, denial of service (DoS), crackers, malware, and phishing. For instance, Ferrag et al. [87] leverage large language models (LLM) such as bidirectional encoder representations from transformers (BERT) in IoT devices to detect cyber threats. Privacy-Preserving Fixed-Length Encoding (PPFLE) techniques were integrated with a Byte-level Byte-Pair Encoder (BBPE) Tokenizer to enhance security and privacy. The result revealed that it takes a central processing unit (CPU) and a compact model size of 16.7 MB and less than

0.15 s to execute, making considerable use in real-time detection of cyber threats in the Industrial Internet of Things (IIoT). Nevertheless, more is required to integrate Security BERT in automated patch management, port management, and antivirus management. Narmadha & Varalakshmi [88] implemented homomorphic encryption, secure multi-party computation, and differential privacy-based federated learning in healthcare. This addresses the persistence of privacy threats. However, more authentication mechanisms, such as blockchain and secure federated learning models, are required to improve data privacy against cyber threats.

4.1 Growing adoption of mobile healthcare applications and security challenges

The delivery of healthcare has been completely transformed by the increasing use of mobile healthcare (mHealth) applications, which allow for real-time health tracking, remote patient monitoring, and smooth patient-provider communication. However, serious security challenges or cyber threats have been brought about by this evolutional expansion of mHealth. Because mHealth apps frequently handle private patient data, such as biometric data and medical history, they are usually the focus of hackers and intruders. Because mHealth systems are dynamic and decentralized, and they involve a variety of devices and networks, they are more susceptible to threats including malware, unauthorized access, data breaches, data privacy, authentication, malware threats, and stringent privacy laws like GDPR and HIPAA apps [23, 26, 89]. To overcome these definite challenges and preserve patient data while keeping confidence in mHealth systems, an enhanced decentralized framework, scalable, and privacy-preserving cybersecurity solutions are needed. The growing adoption of mHealth applications and security challenges is depicted in Fig. 3.

4.1.1 The common cyber threats to mHealth

Figure 3 diagrammatically shows the common cyber threats peculiar to mHealth: DoS/DDoS, Crackers, Phishing, Hackers, Malware, Ransomware, Data Breaches, and Insured APIs. The lapses in security to protect the patient's sensitive data motivate cyber threats to increase. The common cyber threats for mHealth operations are briefly discussed:

(i) Hacker vulnerability exploitation

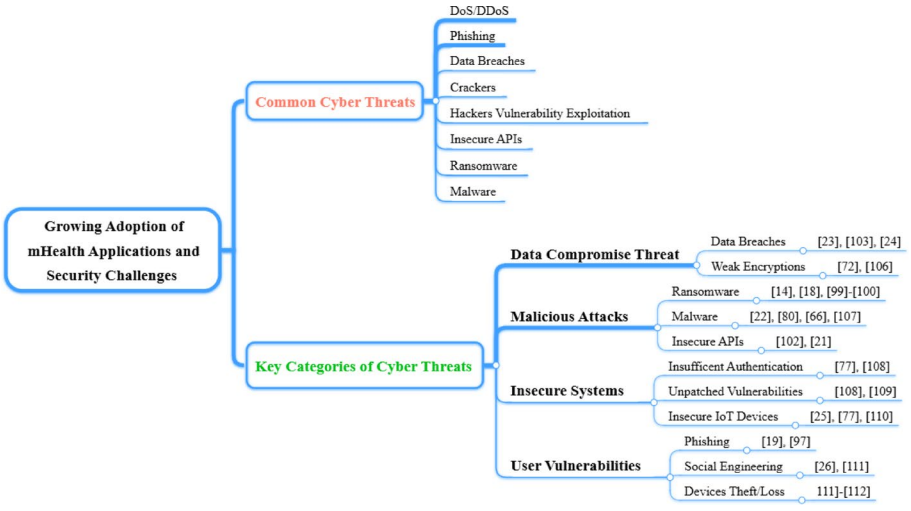

Fig. 3 Growing Adoption of mHealth Applications and Security Challenges

This describes how hackers find and exploit holes or weaknesses in a system, network, or application to obtain unauthorised access, steal confidential information, or interfere with regular business activities [86, 90]. This is sometimes referred to as "state-sponsored actors" [16, 31]. These weaknesses may be caused by inadequate security procedures, out-of-date software, incorrectly configured systems, or code mistakes. Hackers frequently utilise tactics and methods, including social engineering to trick users into disclosing access credentials, exploiting known software flaws (such as through unpatched systems), and scanning for open ports. Once exploited, these flaws can facilitate ransomware attacks, malware injection, and data breaches, putting people and businesses at serious risk, especially in industries like healthcare that deal with sensitive data. In addition, a hacker or other malevolent actor could make the network's entire data-sharing procedure impossible if they successfully breach the central authentication database [90].

For instance [91], distinguished between hackers and ethical hackers based on penetration testers. Indeed, health data is essential to the healthcare industry as well; when hackers use ransomware to block access to this data, the entire process is stopped [92]. highlighted the major causes of hackers' penetration into healthcare environments, which include interjectory of management, technical, and human. However, through blockchain, authentication procedures may be essential to resolving this issue and standardising security hardening in smart cities. Blockchain is a distributed ledger made up of a peer-to-peer network of interconnected blocks that are synced across all users to enable safe data sharing and management without the need for centralised intervention [93]. A recent study by [94] explored the tenacity of healthcare providers' and practitioners' efforts in tackling hackers' activities. Healthcare experts from a range of medical specialities were chosen using convenience and purposeful selection procedures, and their opinions were recorded for the study. The findings through the data analysis indicated that technological threats, such as hacking and encryption flaws, present greater risks to digital health technologies (DHTs) than physical ones. The study looked at workable ways to protect patient data and stop illegal access to DHTs. To combat DHT security concerns, encouraging practices like encryption, multi-factor authentication, frequent security training, and password resets has shown promise.

(ii) Denial of service (DOS) assault

This is one of the cyber threats that aim to prevent legitimate users from accessing a target system, server, or network by flooding it with excessive traffic or requests [21], [95]. Attackers accomplish this by taking advantage of flaws in the system or overloading the target with requests, which results in service interruptions, slowdowns, or crashes. DoS attacks have the potential to destroy vital mHealth apps, block patient data access, and interfere with vital services like telemedicine in healthcare settings. Traditional DoS attacks only employ one source [21]. Still, Distributed Denial of Service (DDoS) attacks [14] use numerous systems to increase the attack's impact, making prevention more difficult. The cyber threats hinder patient treatment, system security, and dependability. The end-targeted system and any system that the hacker has maliciously exploited and forbidden in the dispersed attack are victims of a DDoS attack [22].

For example, researchers have made brazen efforts to tackle DoS and DDoS attacks on mHealth [96]. implemented Secure, Privacy-Preserving Authentication and Key Agreement Framework for mHealth. Automated Validation of Internet Security Protocols

(AVISPA), a common model checking tool, is used to examine the security features of the suggested framework. The proposed protocol is easy to create and resilient to network-related attacks. However, this work might be expanded to incorporate a congestion approach for first and second identities at every software-defined networking (SDN) layer. It better integrates them at the Internet Protocol layer to increase system efficiency and avoid false alerts. Improved safety and a trustworthy environment are necessary for AVISPA implementation at all SDN layers. In addition [97], further explored the machine learning method by implementing a lightweight approach to detect DoS attacks on mobile-enabled sensor networks. This achieved a 99.5% accuracy percentage with the least amount of overhead when compared to other baseline studies, like random forest. Nonetheless, the study requires further evaluation for generalization in healthcare defence.

(iii) Crackers

Given mHealth, crackers are malicious actors who compromise the security of systems or networks, often exploiting vulnerabilities, stealing sensitive information, or causing harm [98]. They target applications, devices, or networks to gain access to private health records, manipulate medical data, or disrupt service delivery by using techniques like exploiting unpatched software vulnerabilities, bypassing authentication protocols, or injecting malicious code. This can lead to financial losses, compromised patient safety, and data breaches. In addition to undermining user trust, crackers also put healthcare providers and developers under pressure to put advanced security measures in place to protect sensitive mHealth ecosystems.

Although both a cracker and a hacker possess an extensive understanding of computer systems and security, their motivations and moral standards are different. Generally, hackers are moral people who investigate systems to enhance security, create novel fixes, or test weaknesses (e.g., white hat hackers and ethical hackers) [90]. Crackers, sometimes known as black-hat hackers [98], on the other hand, carry out malevolent actions, including evading security measures, stealing data, or interfering with systems for their benefit. Grey-hat hackers, on the other hand, sometimes reveal vulnerabilities without authorization and work within moral and immoral lines. Meanwhile, both names describe people with extensive technological knowledge; hackers work to safeguard and improve cybersecurity, while crackers take advantage of it for harmful or unlawful ends. For instance [99], investigated the essence of active defense in healthcare against crackers and other state actors. The results of this study are intended to bolster the argument that, in order to effectively safeguard health information, the healthcare industry may gain a great deal from using active cyber defence (ACD) in its security strategy.

(iv) Malware

A serious cyber threat to mHealth systems is malware, often known as malicious software, which is made to penetrate and harm devices, steal confidential information, or interfere with normal business processes [23, 86]. Apart from malicious software, phishing scams, or infiltrated networks, malware can infect smartphones, wearable technology, or cloud-based platforms inside the mHealth ecosystem. Once inside, malware might alter medical data, remove private patient records, or disable devices, endangering patient safety and service provision. Common forms of malware include spyware [100], which secretly gathers private data, and ransomware [14], which encrypts data and demands payment to unlock it. Malware's attack surface is increased by the development

of connected devices in mHealth, underscoring the necessity of strong cybersecurity measures, including frequent software updates, endpoint protection, and user awareness, to lessen this attack.

Severally studies have been carried out to investigate malware activities or the impact of malware in mHealth. For instance [99], noted that in 2016, the Arizona service provider Banner Health fell victim to a malware attack. The attackers used the "payment processing system" of the food and beverage interfaces to access the company's network, and it took nearly a month for the breach to be discovered. The private information of 3.6 million users was stolen, which cost $6 million. Ullah et al. [85] detected mobile malware in the healthcare sector using multi-model image representation and word2vec-based transfer learning. The suggested approach leverages the benefits of both forms of network traffic by combining their textual and textural properties. Two standard datasets, CIC-AAGM2017 and CICMalDroid 2020, which include 3.2 K benign and 10.2 K malware samples overall, are used to test the suggested approach. However, the study requires further testing, especially using explainable AI [101] experiment.

(v) Phishing

This cyber threat targets mHealth users and systems by tricking people into disclosing private information, like patient data or login passwords [20, 102]. Phishing attacks are typically conducted through phoney emails, messages, or websites that imitate trustworthy organisations, and take advantage of human error to obtain unauthorised access to cloud platforms, electronic health records, or mHealth applications. Successful phishing in the context of mHealth has the potential to endanger patient privacy, facilitate data breaches, or interfere with medical services. For example, a healthcare professional may inadvertently click on a malicious link, giving hackers access to vital systems [20]. Users are especially susceptible to phishing efforts due to the growing usage of mobile devices for healthcare, underscoring the necessity of robust authentication procedures, user education, and cutting-edge email filtering technologies to lower the threat of such assaults. Black Hat hackers use a variety of strategies, including DDoS attacks, phishing attacks, malware development, and social engineering [98].

The attacks have created unprecedented research in the subject areas. For instance [94], designed a structured questionnaire to gather information from medical experts regarding potential phishing security risks, the severity of technical and physical threats, and the degree to which staff and vendor actions impact the DHTs currently used at the University of Cape Coast's Teaching Hospital. The research investigated practical methods to protect patient data and stop illegal access to DHTs. Supporting practices that have shown promise in tackling DHT security concerns include encryption, multi-factor authentication, frequent security training, and password updates [103]. investigated phishing attacks among the healthcare staff. The study adopted quantitative and qualitative survey methods. The results of the attack also revealed that 61% of the targeted healthcare personnel were vulnerable, with some healthcare personnel escaping the attack because they put patient care first and were immune to the phishing attack. However, improved security training and an additional workload-balancing layer of security measures in emergency rooms were recommended to improve staff members' considerate care behavior.

(vi) Ransomware

Malicious software known as ransomware poses a great danger to mHealth systems by encrypting data or locking users out of devices and then requesting a ransom to unlock the device [14]. Files on a compromised device are corrupted by crypto-ransomware, which then demands a ransom to restore them [104]. In the context of mHealth, it can target linked medical devices, mobile health apps, or patient data, interfering with essential healthcare services and endangering patient safety. For instance, during a medical emergency, an assault could disable access to electronic health records or make a wearable gadget unusable [19]. Ransomware frequently propagates via malicious websites, phishing emails, or software flaws. Attackers looking for rapid rewards find mHealth systems appealing due to the sensitive nature of healthcare data and the urgency of medical services.

For example, Sullivan [19] is concerned about ransomware, but it is still a constant threat to healthcare institutions. The percentage of respondents who think their companies are at risk of a ransomware attack has dropped from 64 to 54%. Organisations with ransomware attacks (59% of respondents) reported an average of four attacks over the previous two years (2022–2023). Although fewer businesses paid the ransom (36% in 2024 vs. 40% in 2023), the average amount paid increased by 1.0% to $1,099,200 from $995,450 the year before 2023. Therefore, strong cybersecurity measures are needed to combat ransomware, including frequent data backups, endpoint security, phishing risk education for employees, and deploying advanced detection technologies to find and stop threats before they do damage. In addition, the frequency and sophistication of cyberattacks on agencies that provide health care are rising. Dameff [105] analyzed the number of patients in an emergency department (ED) and the metrics related to stroke care during a month-long ransomware assault on a distinct but nearby healthcare delivery organization. The result shows that there is a substantial rise in confirmed strokes (22 vs. 47; $P=.02$) and stroke code activations during the attack period as compared to the preattack phase (59 vs. 102; $P=.01$). These findings imply that targeted hospital cyberattacks ought to be regarded as a regional disaster since they may be linked to interruptions in the provision of healthcare at nontargeted hospitals in a community. A study by [106] explored the trends of ransomware incidents at US clinics and supported mobile services between 2016 and 2021. Nearly 42 million patients' PHI were made public by 374 ransomware attacks on US healthcare delivery institutions between January 2016 and December 2021. The yearly number of ransomware assaults more than doubled from 43 to 91 between 2016 and 2021. The provision of healthcare was disrupted in over half (166 [44.4%]) of ransomware attacks; frequent disruptions included ambulance diversion (16 [4.3%]), scheduled treatment cancellations (38 [10.2%]), and electronic system outages (156 [41.7%]). Large businesses with numerous locations were more frequently impacted by ransomware attacks on healthcare delivery organizations between 2016 and 2021 (annual marginal effect [ME], 0.08; 95% CI, 0.05–0.10; $P<.001$). However, the minimal information provided by recent monitoring and reporting initiatives may be expanded to provide a more comprehensive picture of how this expanding type of cybercrime impacts mobile healthcare delivery.

(vi) Insecure Application Programming Interfaces

The insecure application programming interfaces, otherwise termed as "Insecure APIs) has contributed to the common cyber threats affecting the effectiveness of mHealth delivery. A defined set of guidelines known as an API makes it possible for various apps

to speak with one another [107]. The same discipline must be applied to application programming interfaces (API) that link enterprise apps and data to the cloud because they are vulnerable to the same threats as standard cloud-based apps. The unidentified attackers obtain important data about the security token of the Rivest-Shamir-Adleman (RSA) algorithm—a device that creates one-time keys to improve online security—by using secure APIs [22]. APIs are being used by businesses more and more to link services and move data, including private, sensitive financial, and medical information.

Several studies have revealed how insecure APIs have contributed to attacks on digital devices such as mobile phones and smartphones. According to Bob [107] discusses the crucial role of APIs in companies' digital transformation initiatives, following 57% of respondents. However, organizations run the risk of experiencing a significant security breach when they use APIs that have vulnerabilities. The report revealed that in 60% of respondents, at least one data breach resulting from API exploitation had occurred in their organizations. IP theft and financial loss were the outcomes of several of these breaches. In addition, through insecure APIs, security concerns can be generated, provide a getaway for attackers and most importantly, when this security is not checked/considered during API design. This is often associated with misconfiguration of APIs, and operational disruptions are evident because of insecure APIs.

(viii) Data Breach

A data breach happens when private health information, like patient IDs, medical records, or personal health information, is accessed by unauthorized people or organizations [24, 108]. In mHealth, this frequently entails breaking into servers, cloud storage, or mobile health apps that store private information. Businesses have different plans for dealing with the rising cost and frequency of data breaches, according to IBM research from 2023 [107]. While 95% of the firms surveyed reported having multiple breaches, the study also indicated that breached organizations were more inclined to pass event costs on to customers (57%) than to boost security investments (51%). Based on a thorough examination of actual data breaches that occurred at 553 companies worldwide between March 2022 and March 2023, the 2023 Cost of a Data Breach Report was created. The Ponemon Institute carried out the study, which IBM Security financed and assessed, and it has been published for the past 18 months [107]. However, from the study, we can deduce that the 2023 IBM report is greatly impacted, and improvement can be achieved through AI picking up speed, detection gaps, and the cost of silence. Nevertheless, constantly using cybersecurity solutions and AI-based algorithms such as k-Nearest Neighbor (kNN), decision tree (DT), random forest (RF), and other advanced methods, such as blockchain-based technology and federated learning for traffic analysis to overhaul eavesdropping cyber-attacks, especially internet traffic, which may be perceived to be lawful or harmful [25].

Furthermore [109], utilized fuzzy-based techniques to analyze the breaches in healthcare data, especially in the advent of the COVID-19 pandemic. The results show that about 12 billion records from 2005 to 2021 were exposed in many industries such as medicine, education, non-governmental organizations (NGOs), government, etc. There have been 4371 recorded significant data breaches in the healthcare sector alone. Approximately 85% of health data was compromised between 2020 and 2021, which is the greatest percentage of any industry. The frequency of hacking/IT incidents increased by 37.22% between 2020 and 2021. However, theft/loss, improper disposal, and unlawful

internal disclosure decreased by 29.88%, 31.94%, and 22.22%, respectively, between 2020 and 2021. Nevertheless, the study lacks the development of a theoretical framework. In addition [110], investigated what to do after recording a data breach incident. How should a data breach be handled? The study offers compensation and apology as reaction tactics for healthcare providers. Healthcare providers should ascertain the particular demands of their clients and adjust their data breach recovery plans accordingly.

4.1.2 The key categories of cyber threats for mHealth settings

As shown in Fig. 3, the cyber threats are grouped into key categories based on their operational nature and the methods used by attackers. These include data compromise, malicious attacks, insecure systems, and user vulnerabilities. Data compromise threats include data breaches and weak encryption. Malicious attacks are ransomware, malware, and insecure API threats. Insecure systems comprise insufficient authentication, unpatched vulnerabilities, and insecure IoT devices. In addition, user vulnerabilities consist of phishing, social engineering, and device theft or loss. The categories, descriptions, causes, and impacts of cyber threats for mHealth settings are presented in Table 3.

4.2 Mitigation strategies to cyber threats in mHealth settings

It is essential to provide mitigation strategies to address the common cyber threats, inherent causes, and impacts on mobile healthcare applications. It required multi-layered methods combining organizational, technical, and regulatory strategies. In this study, we identified five mitigation strategies including their approaches for comprehensive solutions. The mitigation strategies to cyber threats in mHealth apps are represented in Fig. 4.

4.2.1 Robust security practice

This involves effectively implementing behavioral analytics, zero trust architecture, blockchain-based technology, and AI-based threat detection. Strong security procedures are essential for safeguarding sensitive health data in mHealth applications. Confidentiality and integrity of health records are protected by encryption, which builds trust among users who depend on mHealth platforms to manage personal health information. Data encryption, especially with advanced protocols like AES-256, guarantees that sensitive information stays safe both during transmission and at rest, preventing unauthorized access even if data is intercepted [116–118]. Also, secure authentication techniques [118, 119] such as multi-factor authentication (MFA) significantly improves security by demanding several kinds of verification before allowing access. By introducing an extra layer of protection, MFA lowers the possibility of unwanted access, even if login credentials are stolen. For instance, ensuring that only authorized users can access sensitive data involves combining a password with a biometric verification method, such as a fingerprint [26]. This precaution is especially crucial in mHealth contexts, where data breaches can have serious privacy and legal repercussions. In addition, finding and fixing flaws in app architecture requires routine security audits that include code reviews and penetration testing. Developers can proactively identify vulnerabilities that hackers might exploit thanks to regular security audits [120]. Organizations may maintain a solid security posture and adjust to changing threats by implementing a continuous audit cycle. These procedures work together to create a thorough plan for defending mHealth

apps against online attacks. In addition, ensuring government implementation of policies and strategies for effective healthcare services to alleviate the burden of the patients and training of rural patients based on users' data safety [121].

For example [122], implored a deep, convoluted learning framework approach to address security concerns in smart healthcare. The framework has a high degree of accuracy in detecting cyberattacks, and several important performance indicators are used to evaluate performance. However, further usability study is required for generalization. The lack of usability and accessibility of smart healthcare systems, such as mobile devices, especially by older people, mostly contributed to the lack of security lapses [73]. utilized AI-powered chatbots to increase elderly folks' access to and usage of healthcare smart devices. Therefore, the study uses an iterative method based on direct user feedback, enabling the overcoming of such limitations and the provision of healthcare services that were needed by the target group of older persons.

4.2.2 User education and cyber hygiene

This method includes awareness campaigns, guidelines for sage usage, and privacy-setting tutorials. One of the most important ways to improve the security of mHealth apps is to educate users about cybersecurity threats [27, 123]. To enable users to identify and steer clear of possible assaults, awareness campaigns seek to educate them about prevalent risks, including phishing and social engineering. These ads decreased the risk of account penetration, highlighting the significance of safe measures like making strong passwords and avoiding credential reuse. Also, by giving precise guidance on how to download software exclusively from reliable sources and spot questionable activity, safe usage guidelines further reinforce secure practices [124]. Users are advised, for example, to avoid downloading programs from unapproved marketplaces and to confirm the legitimacy of app creators. By reducing their exposure to cyber threats, these rules assist users in safely navigating the digital world. Moreover, users can efficiently configure their accounts with the help of privacy settings lessons provided within mHealth applications [125]. These lessons improve privacy and lower data exploitation by teaching users how to manage permissions and restrict data sharing. Users become active participants in preserving cybersecurity when they are taught the value of privacy settings, which cultivates a sense of control and accountability. For example [126], presented an empirical investigation of end users' security awareness about mobile health applications. Saudi Arabian mHealth providers collected information from 101 end customers. The empirical findings highlight the need for mHealth providers to embrace appropriate mHealth apps (e.g., security vs. usability trade-offs), encourage best practices to enforce security (e.g., multi-step authentication), and guarantee end-user security training (e.g., threat analysis workshops).

In addition, cyber hygiene improved the safety of digital environments through the use of a set of rules and appropriate measures to protect personal information and prevent cyber threats [127]. In higher institutions/education, especially in the Internet of Medical Things (IoMT), cyber hygiene awareness is raised to protect users against cybercriminals/cyber threats and the development of the capability of the patient, health professionals, educators, researchers, and students to apply caution to safeguard their digital resources. For instance, Khanna [128], developed an effective cyber hygiene framework that assisted in integral management to prevent data breaches and sensitive

Table 3 Categories, descriptions, sources, and effects of cyber threats for mHealth settings

Categories	Methods	Descriptions	Causes	Impacts	Author
Data Compromise Threats	Data Breaches	It often entails breaking into servers, online storage, or mobile health apps that store sensitive data	- Weak access controls (e.g. weak passwords) - insecure cloud services/misconfigured settings	- Loss of patient confidentiality. - Legal consequences (e.g., violations of HIPAA or GDPR). - Reputation damages to mHealth providers	[24, 25, 110]
	Weak Encryption	Sensitive health information that is not adequately encrypted, either while it is being transmitted or stored	- Outdated encryption protocol usage - Failure to encrypt data during transmission over unsecured networks (e.g., public Wi-Fi)	- Exposure of private health data during transmission. - Increased risk of data theft	[76, 111]
Malicious Attacks	Ransomware	Encrypts files rendering the health information inaccessible until a ransom is paid to the attacker	- Phishing emails or malicious links - Unpatched vulnerabilities in software	- Loss of access to critical health data and breach of patient care continuity - Major financial loss due to recovery efforts or deal payments	[14, 19, 107, 108 106]
	Malware	A malicious app is designed to damage a device or network. E.g., viruses, trojans, and spyware. In mHealth, malware can infect devices or apps to steal personal health data, spy on user behavior	- Unknowingly downloading infected apps - Clicking on malicious links or compromised website	- Theft of sensitive health data. - Unauthorized or compromised user account access - Financial loss or operational disruptions for healthcare operators or professionals	[23, 86, 100] [112]
	Insecure APIs	mHealth apps' APIs are weak areas that let hackers exploit vulnerabilities during data exchange between systems. Due to third-party services integration	- Lack of proper authentication and authorization in API endpoints. - Nonexistent input validation in API calls. - Unencrypted API traffic	- Manipulation of sensitive health data. Exposure of data, especially if APIs are misused.	[22, 109]

Table 3 (continued)

Categories	Methods	Descriptions	Causes	Impacts	Author
Insecure Systems	Insufficient Authentication	Weak methods for confirming users' or devices' identities before allowing access to private health information. E.g., readily guessed passwords, not implementing multi-factor authentication (MFA), or focusing on passwords only	- Use of single-factor authentication - No advance user verification identity beyond the initial login.	- Unauthorized access to sensitive data. - Misuse of health data or Identity theft	[82], [113]
	Unpatched Vulnerabilities	This involves security flaws in the underlying software of mobile apps that have not been considered through patches or software updates	- Failure to regularly update and patch apps and systems - Absent security fixtures from developed apps	- It increases the high risk of exploitation by cyber attackers - Leads to loss of data integrity	[113, 114]
	Insecure IoT Devices	Wearables, health monitors, and connected medical equipment are examples of IoT devices that, if not adequately secured, might be subject to cyberattacks. Hackers target these devices because they often gather and send health data.	- Insecure communication (e.g., no encryption). - Weak default passwords - Lack of regular firmware updates	- Compromise of device functionality. - Unauthorized manipulation of health readings - May cause major harm to patients, especially if systems are altered with	[26, 82, 115]
User Vulnerabilities	Phishing	Attackers pretend to be trustworthy entities (such as medical professionals or developers) to trick users into divulging private information, like login passwords or health information.	- Deceptive emails, SMS messages, or phone calls. - Fake websites that resemble legitimate healthcare websites.	- Unauthorized access to health data. - Leads to financial loss due to fraudulent activities - Compromise of user login details or identity.	[20, 104]
	Social Engineering	It coerces people into revealing private information or taking security-compromising acts. In the context of mHealth, it deceives users into giving sensitive health information and granting app permissions	- Lack of awareness and training on cybersecurity best practices. - Trust in unknown contacts	- Theft of sensitive data - User error due to breaches in security - Vulnerability to additional assaults, including identity fraud or credential theft	[27, 116]
	Device Theft or Loss	A mobile device carrying private health information (or login credentials) is misplaced, posing a serious security risk. Attackers may gain access to the device's data if it is not properly secured (e.g., with strong passwords and encryption,).	- Lack of device-level security - Inability to utilize remote wipe or location-tracking features.	- Exposure of sensitive health data - Unauthorized access to mHealth services - Financial damage	[116, 117]

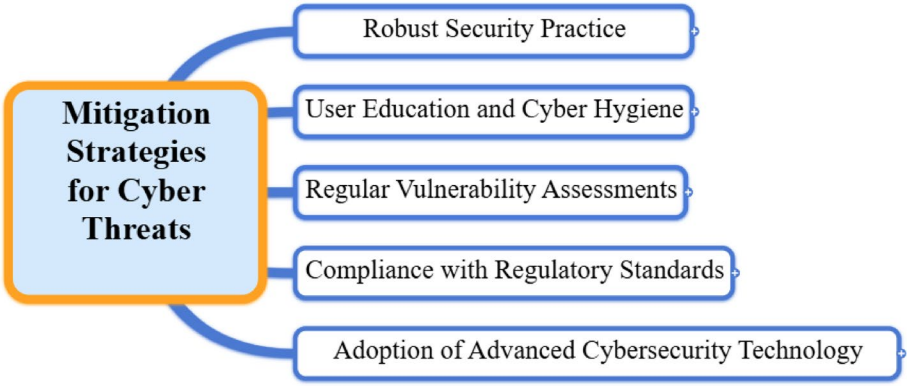

Fig. 4 The mitigation strategies to cyber threats in mHealth apps

information. The study provides all necessary policies and procedures that enable meaningful results for cyber hygiene, which are engineered through education, training, and automation. Nonetheless, there is still a lack of awareness of cyber hygiene and cybersecurity in the contemporary digital environment. Cyber hygiene has contributed to reshaping the cyber-connected device from an attack through education and training. Researchers have embraced this phenomenon. For instance, Surdjono [129] maintained that utilizing mobile-based learning will improve cyber hygiene for cybersecurity awareness activities to work effectively. The study added to raise awareness in key sectors such as finance, healthcare, and accounting for addressing the inherent issues of cyberattack vulnerability. Nevertheless, exploring the program's applicability in other sectors through education and training campaigns is necessary.

4.2.3 Regular vulnerability assessments

This approach ensures that proactive threat hunting, patch management, hand gesture recognition, and continuous monitoring of suspicious activities in the system [33, 86, 130, 131]. Finding and reducing any security threats in mHealth applications requires vulnerability evaluations. In proactive threat hunting, vulnerabilities in servers, mobile app code, and APIs are scanned using both automated technologies and manual methods [27, 132]. Organizations can identify and fix vulnerabilities with this method before they are taken advantage of. Proactive evaluations improve the overall security architecture of mHealth platforms by anticipating possible threats. Patch management [133] is another crucial component of vulnerability mitigation. Making sure that software components receive timely updates and patches, fix known vulnerabilities and stop hackers from taking advantage of out-of-date systems is crucial. In mHealth settings, where vulnerabilities can compromise sensitive health data, it is especially critical to update operating systems, third-party libraries, and app software regularly. This practice improves security and shows a commitment to user safety and regulatory compliance. Additionally, real-time insight into network activity is made possible by ongoing monitoring using intrusion prevention systems (IPS) and intrusion detection systems (IDS) [59, 80, 86, 134]. These systems examine network traffic to spot irregularities and react quickly to possible dangers. Organizations can guarantee the continuous safety of sensitive health information by preventing data breaches and detecting unwanted access attempts through the implementation of IDS and IPS. When combined, these steps give mHealth apps a proactive and dynamic security approach.

Furthermore, some of the studies that utilize this strategy for cyber threat mitigation in mHealth are briefly highlighted. For example [110], investigated what to do after recording a data breach incident. How should a data breach be handled? The study helps healthcare providers ascertain the particular demands of their clients and adjust their data breach recovery plans accordingly [118]. introduced a lightweight hybrid federated learning framework where blockchain smart contracts control the distribution of globally or locally trained models, the reputation of edge nodes and their uploaded datasets or models, the edge training plan, trust management, and authentication of participating federated nodes. Additionally, the system facilitates the inferencing process, model training, and complete dataset encryption. The blockchain aggregates the updated model parameters via multiplicative encryption, while each federated edge node carries out additive encryption. The results show a wider adoption of the Internet of Health Things (IoHT) for the security of health management data. In addition [135], Implemented cyberattack anomalies in IDS management using deep learning based machine learning methods. However, the study requires further investigation to evaluate identity privacy via an intrusion detection system, especially in healthcare systems.

4.2.4 Compliance with regulatory standards

To ensure cyber threat detection practice and safety towards the implementation of mHealth, compliance with security and regulatory standards is an important step. The two major regulatory standards include the General Data Protection Regulation (GDPR), which is based on the European Union (EU) [115, 136] and Health Insurance Portability and Accountability Act (HIPAA) based United States of America (USA) [137–139]. It also includes third-party risk management [140] and data anonymization adherence [141]. For mHealth applications to guarantee data security and legal compliance, regulatory standards compliance is a necessity. Implementing strict data protection procedures, such as getting user consent for data collection and ensuring data storage is safe, is necessary to comply with standards like GDPR and HIPAA. By offering a methodical approach to handling private health data, these rules promote confidence among stakeholders and users. Maintaining compliance also requires third-party risk management. To make sure third-party providers follow the same security and privacy guidelines, organizations need to screen and keep an eye on them. This involves evaluating the data security, encryption, and access control procedures used by vendors. Organizations can avoid supply chain vulnerabilities and preserve a safe environment for mHealth applications by controlling third-party risks. By safeguarding user identities, data anonymization strategies like data masking and pseudonymization improve compliance even further. By using these techniques, businesses can gain insights from data analysis without exposing the privacy of individuals. mHealth platforms can comply with regulations and guarantee the confidentiality of sensitive health data by incorporating anonymization into their data management procedures.

For instance [114], explored the development of cybersecurity medicine, guarding implanted technology against online attacks. The study highlighted the importance of regulations and compliance with health standards in curtailing cyber threats in mHealth. The study further maintained that regulatory agencies are realizing how important it is to include cybersecurity specialists in the supervision of linked medical devices. When evaluating the safety of new devices, the Food and Drug Administrator (FDA) has

indicated that it will seek advice from cybersecurity experts. Their advice helps strike a balance between patient needs and product security, enabling life-saving innovation to move forward with the right safeguards. However, a niche from the government would be necessary to create grants that accelerate more development and a transparent regulatory framework in the healthcare industry.

4.2.5 Adoption of advanced cybersecurity technology

This involves the leverage of advanced technologies such as AI-based such as machine learning [60, 63], blockchain [59, 142], zero thrust architecture [143, 144], and behavioural analytics technology [112]. Real-time threat detection capabilities offered by artificial intelligence (AI) and machine learning (ML) are transforming cybersecurity. These technologies examine enormous volumes of data to spot trends and abnormalities that could point to malicious activity, like odd login attempts or requests for unauthorized data access. AI, in contrast to conventional techniques, can evolve and learn from new threats over time, increasing the accuracy of detection [60, 63]. By taking a proactive stance, organizations can reduce response times and address threats before they become serious breaches. AI-powered solutions provide a vital line of defence against increasingly complex cyberattacks in mHealth environments, where private health information is at risk. Also, AI-based threat detection systems can be easily integrated with other security solutions to offer a comprehensive protection approach. To help security teams concentrate on the most important vulnerabilities, they can, for example, rank threats according to their seriousness. More so, by reducing the need for manual monitoring, these technologies free up resources for other crucial duties. Applications for mHealth can avoid new risks by utilizing AI and ML, guaranteeing the ongoing security of private health data.

Additionally, unmatched security is provided by blockchain technology for handling and storing private medical data. Data cannot be changed or removed without network participants' consent because to its decentralized and unchangeable nature. Because it removes the possibility of unwanted changes, blockchain is the perfect way to preserve the integrity of medical records. Blockchain's openness also makes it possible for transactions to be tracked and verified, offering an auditable record of data access and changes. This guarantees patient data security in mHealth applications while upholding accountability. Blockchain can improve consumer privacy in addition to data veracity [59, 142]. Blockchain makes it possible to share data securely without disclosing private information by employing cryptographic techniques. Patients can temporarily authorize access to healthcare professionals, for instance, without disclosing all of their medical history. In addition to improving privacy, this fine-grained control over data access fosters user trust. Blockchain technology can provide strong security and privacy features that meet user expectations and regulatory requirements as mHealth applications use it.

The security system known as Zero Trust Architecture (ZTA) [143, 144] is based on the tenet "never trust, always verify." ZTA demands authentication and authorization for each access request, independent of the user's location or device, in contrast to conventional security models that presume confidence within a network perimeter. In mHealth situations, where users often use applications from several devices and places, this strategy works very well. ZTA reduces the possibility of insider threats and illegal access by confirming each access attempt. ZTA implementation incorporates technologies such

as continuous monitoring, micro-segmentation, and multi-factor authentication (MFA). These safeguards make guarantee that even if one area of the system is compromised, other areas are not affected. This fine-grained control over access improves security for mHealth applications without sacrificing user experience. ZTA offers a strong framework for protecting sensitive health data from internal and external attacks as cyber threats continue to change. Furthermore, by examining variables like login times, device usage, and data access patterns, behavioral analytics can spot anomalies that could point to compromised accounts or insider threats [112]. For instance, if a user who usually logs in from one location suddenly accesses the system from multiple locations in a short amount of time, the system can flag this behavior as suspicious and initiate additional verification steps [145]. Behavioral analytics is centered on finding unusual patterns in user behavior to detect potential security threats. Because behavioral analytics provides real-time insights into user activities, it helps organizations respond quickly to potential threats. Additionally, behavioral analytics can be integrated with other cybersecurity tools to create a comprehensive defense strategy. As mHealth platforms adopt behavioral analytics, they gain a powerful tool for mitigating risks and ensuring the security of sensitive health data. Behavioral analytics is beneficial in mHealth applications for detecting subtle threats that traditional security measures might overlook, such as irregularities in the typical behavior of an insider trying to access restricted patient records.

5 Cyber threat detection approaches in mobile healthcare application

Cyber threat detection (CTD) in the mobile healthcare sector is essential. By improving accessibility and efficiency, mHealth systems have completely changed how healthcare is delivered. However, they are vulnerable to a complicated and constantly changing array of cyber threats because they rely on interconnected networked devices and cloud-based systems [56, 66]. Due to the sensitive nature of patient data and operations, Healthcare facilities are prime targets for cyber threats or attacks. Thus, comprehensive threat detection mechanisms are trivial. This section briefly discusses traditional and contemporary approaches, as well as centralized and decentralized detection approaches to cyber threat detection mHealth environment, followed by centralized and decentralized systems.

5.1 Traditional and contemporary

This section discusses the traditional and contemporary cyber threat detection approaches.

5.1.1 Traditional approaches to cyber threat detection

A well-known application of traditional methods deployed to detect cyber threats includes (a) signature-based detection, (b) perimeter defence, and (c) manual log analysis. Signature-based detection is called misuse detection, which employs database patterns of known attacks [82, 146]. The patterns in the form of a sequence of bytes are compared with the database when they are matched. Signature-based has higher accuracy and can thoroughly examine packet information. However, it lacks the scalability and search capability to identify modern assaults. A conventional cybersecurity strategy called “perimeter defence” aims to erect a wall between an internal network and outside threats in 2024 [147]. It helps to monitor, filter, and manage incoming and outgoing

traffic, solutions such as firewalls, intrusion prevention systems (IPS), and virtual private networks (VPNs). The goals of these defences are to shield internal systems from outside threats and stop unwanted access. For example, consider a game situation where the intruders seek to reach the perimeter without being caught by the defenders, while the defenders are restricted to moving along a perimeter and attempting to capture the intruders [147]. Perimeter defence is not enough in the framework of mobile healthcare, because data and devices typically operate outside of conventional network perimeters. It must be combined with more flexible and dynamic methods. Additionally, manual log analysis (MLA) is the process by which human professionals or experts examine systems, applications, or network logs to spot odd or suspicious activity that might point to a cyber threat [33, 148]. MLA was mostly used in the early 2000 s when security teams analyzed network data and system event logs using stochastic approaches [149]. Logs provide important information about any weaknesses or breaches by capturing specifics like login attempts, system problems, and data access patterns. Considerably, MLA is best compared to signature-based and perimeter-based detection, because of a supplementary tool, supporting automated threat detection methods for comprehensive cybersecurity in dynamic and distributed healthcare environments.

For instance, some studies have utilized this traditional approach to resolve cyber threats in mHealth environments. A study by Rabie et al., [150] implored certificate-less aggregation signature-based authentication to enforce privacy-preserving in healthcare smart wearable systems, which reduced the computational cost by 93%. The study eliminates the need for a centralized medical server for verification. However, an advanced privacy and security-based mechanism, such as artificial intelligence, is needed [151]. utilized signature encryption to detect threats in cloud computing, enabling mobile medical services. To make sure the solution is reliable, collaborate with third-party audits and concentrate on privacy-enhancing technologies. The cloud computing-based signature scheme offers significant security and performance benefits, can satisfy data protection and privacy requirements across several industries, and has a broad range of potential applications. However, traditional approaches are no longer sufficient to address the cyber threat in the healthcare system due to the dynamic and interconnected nature of threats evolving rapidly and often bypassing static defences. Hence, contemporary approaches for CTD in mHealth care environments. The traditional approaches, descriptions, weaknesses, and strengths are presented in Table 4.

Table 4 Traditional approaches, descriptions, weaknesses, and strengths

Traditional Approaches	Description	Weakness	Strength	Reference
Signature-based detection	It matches patterns in traffic/files against a malware signature in the database	Ineffective against zero-day threats, advanced persistent threats (APTs), and limited search capabilities	Simple to develop, effective against known threats	[45, 82, 146]
Perimeter defence	Provide firewalls and network access control (NAC) systems to establish barriers to prevent unauthorized access	Lacks visibility into encrypted traffic and is not effective for mobile and cloud-based systems. Also, ineffective for mobile/decentralized settings	Enable basic protection for internal systems and easy-to-deploy	[147, 152] [147, 152]
Manual log analysis	Involves manual review of system logs that identify anomalies and potential breaches	It takes much time and has scalable issues for modern healthcare environments	Good for post-incident analysis	[33, 148, 149]

5.1.2 Contemporary cyber threat detection approaches

Generally, contemporary methods are all-encompassing, since they offer proactive monitoring (i.e. real-time detection and extenuation), adaptability (i.e. increases volumes of data in healthcare settings), and scalability (i.e. counters new attacks/threats). Therefore, the insufficient pragmatic traditional approaches gave rise to more proactive methods, leveraging advanced analytic methods. The methods include AI and machine learning, endpoint detection and response, threat intelligence sharing, zero trust architecture, and blockchain for data integrity [19, 153]. The contemporary approaches are depicted in Fig. 5.

The contemporary approaches, as depicted in Fig. 5, are described as follows:

(i) AI and machine learning: Artificial intelligence (AI), machine learning (ML) and even deep learning (DL) are major analytics data-driven components in the domain of cybersecurity that are capable of detecting anomalies through behavioural baselines for network devices and users [81, 84, 102]. According to Labu & Ahammed [81] implemented AI, ML, and DL techniques to reinforce the uncovering of fraudulent activities using Feedzai AI-based security software combined with the Random Forest (RF), k-nearest Neighbors (kNN), and Naïve Bayes (NB) algorithms. The study achieved an average accuracy of 83.94% (RF), 78.74% (kNN), and 79.23% (NB). RF with the highest accuracy to detect cyberattacks. A machine's ability to simulate or approximate human intelligence is known as artificial intelligence or AI [25, 154]. The best aspect of artificial intelligence is its capacity to act and reason in a way that optimizes the chances of achieving a desired goal. In this regard, the combination of cybersecurity and artificial intelligence offers a glimmer of hope by offering creative ways to strengthen defences against the ever-changing threat landscape [154]. Artificial intelligence gave birth to machine learning; likewise, deep learning is a subset of machine learning.

AI in cybersecurity is evolving to include adaptive protection mechanisms in addition to threat detection. Systems with adaptive AI incorporated demonstrate the ability to learn from persistent cyber threats and automatically modify security configurations and protocols to reduce new threats [154]. These AI-powered adaptive defences have the potential to strengthen networks' and organizations' resistance against previously unheard-of and highly advanced attacks. AI in cybersecurity offers numerous benefits such as faster detection, network security, phishing detection, secure authentication, behavioral, and preventing online fraud. This is pictorially represented in Fig. 6. However, it has a pyramid of challenges such as a lack of high-quality data for training, and requires enormous computational resources [155]. Another difficulty is that privacy concerns and ethical issues, such as biases in AI algorithms, force a careful approach to the use of AI in cybersecurity [155, 156].

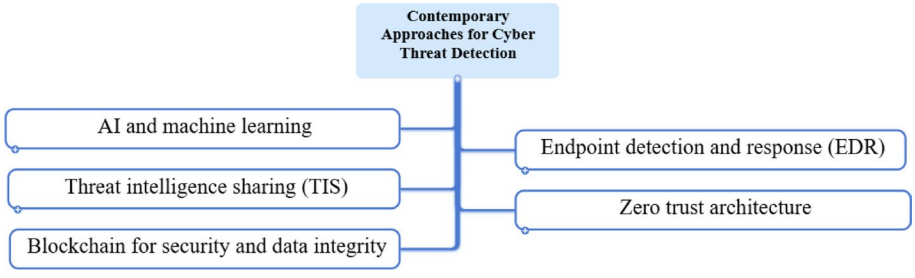

Fig. 5 Contemporary approaches for cyber threat detection

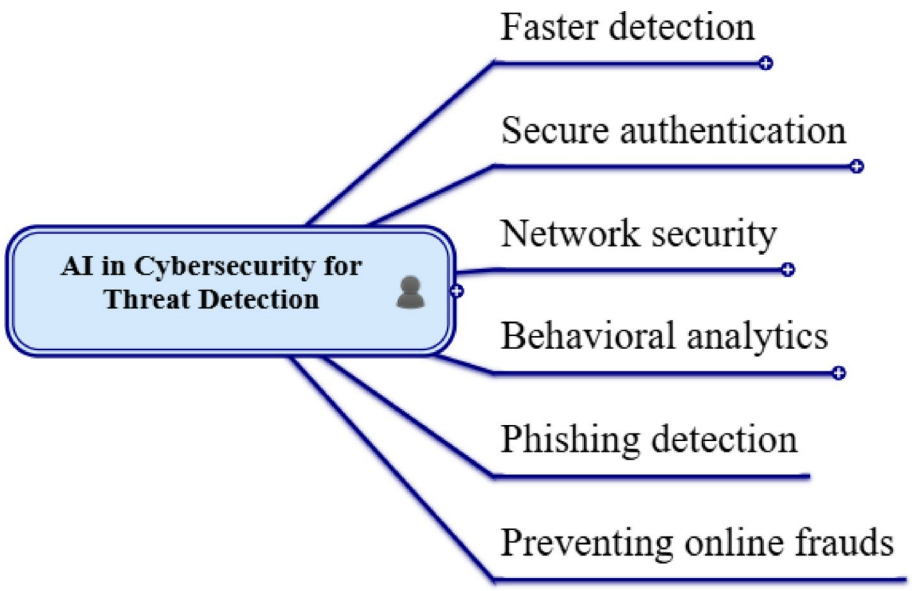

Fig. 6 AI in Cybersecurity for threat detection

Machine learning (ML) as a subset of AI plays a significant role in cyber threat detection. In the realm of cybersecurity, machine learning has become a game-changing instrument. Machine learning allows systems to identify patterns and spot abnormalities that can point to malicious activity by utilizing algorithms that can learn from and make predictions based on data [20, 102]. ML models are especially well-suited for cyber threat identification due to their capacity to continuously evolve and adjust to new threats. ML offers enormous benefits such as real-time analysis, automation, enhanced threat detection accuracy, and adaptive learning [20, 24]. Several studies have used machine learning to detect cyber threat-related cases. For instance, Shaukat et al. [102] evaluated the performance of machine learning techniques such as deep belief networks, support vector machines, and decision trees deployed to detect the most sensitive cyber threats via cyberspace. This proves to be effective for detecting spam, intrusion, and malware using the usual benchmark datasets. Also, research findings show that machine learning enhances cyber threat detection potential [20]. However, the security, privacy, and ethical concerns persisted in the implementation of ML for mHealth environments.

Different machine learning algorithms have been widely implored by numerous authors to detect cyber threats, especially in mobile healthcare services. For example [157], analyzed security concerns in a smart healthcare environment. The study utilized the ensemble algorithms (e.g. Logistic Regression and kNN) for intrusions such as man-in-the-middle (MITM), DDoS, and data injection. The results show a high accuracy of 92.5% for the first dataset and 99.54% for the second, and a precision of 96.74% for the first dataset and 99.228% for the second, the results demonstrated the effectiveness of the suggested ensemble method in identifying intrusion attempts and categorizing them as attacks or regular network traffic. Nevertheless, it is now impossible to ascertain the performance parameters of such an architecture due to the restriction of accessing real-time traffic network data in an environment associated with IoMT. A most recent study by [158] explored machine learning algorithms such as Support Vector Machine (SVM), kNN, Random Forest (RF), and Decision Tree (DT) with deep learning methods to

detect intrusion. The system is reliable and interpretable to effectively detect anomalies in mHealth. However, the study requires further testing with different ensemble models, continuous monitoring and updating, and anomaly detection.

(ii) Endpoint detection and response (EDR): This uses resources from ML applications to monitor endpoints spontaneously, enabling real-time analysis and speeding up response to suspicious practices, to ensure optimal security posture [20, 24]. Endpoints connect to other areas of the network, maintain user account credentials, and contain data. An adversary may use a single endpoint as an exfiltration point, persistence mechanism, or entrance vector. Investing in endpoint-centric solutions, such as conventional antivirus software and EDR systems, is one way that organizations contribute to endpoint security [153]. Endpoint technology is usually the primary focus of security postures, which also frequently incorporates various forms of telemetry to assist endpoints. However, adversaries continue to carry out successful breaches despite the investments made by numerous institutions.

Some important factors for endpoint security, particularly in light of cyber threats, include [153]: (i) Endpoint solutions should leverage emerging technologies such as AI/ML, and moving target defences (MTD); (ii) Security teams should be informed and empowered by endpoint solutions; and (iii) Teams are not given the required edge by merely reporting detections without more context or related information. For teams to use the same platform for triage, analysis, containment, and blocking, endpoint security should be combined with detection and response capabilities. Furthermore, endpoints pose a special threat to businesses because they are [33]: (i) the most prevalent asset type in an organization; (ii) the most desirable target for attackers at different phases of an attack; and (iii) potentially the target of several threats that other security measures are supposed to stop. Nonetheless, despite the proactive and comprehensive measures, the dynamic nature of cybersecurity threats often beats the capabilities of most developed defensive measures.

(iii) Threat intelligence sharing (TIS): Platforms combine threat information from several sources to anticipate and lessen attacks. Threat Intelligence Platforms (TIPs) are specialised software that helps organizations by collecting, correlating, and analyzing real-time threat information from various sources to strengthen their defensive strategies [29]. While there are many TIPs available in the market, the majority are offered under commercial licenses. Historically, organizations relied on informal means such as phone calls and emails to share threat intelligence, but there is a growing trend towards creating connected communities that use dedicated platforms to facilitate the automated or semi-automated sharing of threat intelligence. Sun et al. [86] also identified a new perspective and proactive security defence process for cyber threat intelligence. The method includes perception (scenario analysis and data collection), comprehension (distillation and knowledge acquisition), and projection (performance evaluation and decision-making). The TIS is applied to mobile apps to update the latest threat signatures and intelligence. It is useful for proactive defence against rising threats. Nevertheless, it involves much integration of the infrastructure of mobile healthcare.

(iv) Zero trust architecture: It secures all interaction between backend servers and mobile applications in healthcare settings. The continuous deployment of an enhanced cyber threats detection system, such as advanced persistent threats (APTs) and zero-day attacks, requires more proactive defence methods that are capable of detecting and

mitigating high-level risk occurrences [24]. Zero-Day Exploits express vulnerabilities in software or systems that manufacturers or security professionals are unaware of [33]. Attackers use these flaws to initiate focused attacks undetected by security systems that rely on signatures. According to Sun et al. [143] identified zero-day attack paths using Bayesian networks. The study explores threat-hunting skills, like behavioural analysis, anomaly detection, and intrusion detection, to tackle zero-day defencelessness. However, the study can only reveal paths of the parts of the attacks, but is limited, especially when the generated instance graphs do not fully depict the zero-day attack paths if the attack duration surpasses the analysis duration. Consequently, organisations are usually exposed to zero-day threats and other sophisticated threats that normally take advantage of unknown vulnerabilities or flaws in software and systems [24]. Nevertheless, zero trust architecture is limited to surface threats through segmenting access, and the implementation cost is high.

(v) Blockchain for security and data integrity: It guarantees safe and unchangeable data transfer between mHealth systems and devices [53, 59]. It monitors the exchange of patient data between healthcare providers and wearables. It promotes trust and data integrity [51]. Conversely, it is associated with problems of resource-intensive and scalability implementation. Examining how AI and cutting-edge technologies like blockchain and quantum computing work together could provide fresh ideas for bolstering cyber defences against hitherto unseen threats [154].

The emergence of blockchain applications in cybersecurity to secure the mHealth data of patients has become a reality. A lot of studies have leveraged the blockchain for data security and ensuring data integrity. For instance, Rahman et al. [118] utilised blockchain-based federated learning methods such as differential privacy (DP) to privately secure and enhance Internet of Health Things (IoHT) data in a mobile device, especially during the coronavirus (COVID-19) outbreak. However, it lacks accuracy and average loss. Zhang et al. [159] implemented differential privacy in age-dependent considering the stochastic aspect of a time-changing database. Nonetheless, adaptive composition is required to improve privacy assurance in case of multi-query scenarios. Kang et al. [53] leveraged consortium blockchain to achieve efficient reputation management of organisational employer repudiation and tampering from mobile devices. The metric was represented by the reputation concept to select a reliable employer as proposed in federated learning operations. The result obtained shows two attackers with 76.12%, which is significantly means 7.7% lower than one attack when Earth Mover's Distance is 1.6 and the strength of the attackers achieved 0.9. Nonetheless, how to adjust the reputation threshold dynamically to reduce the harm caused by dishonest employees remains a big challenge. A more recent study by Rehman et al. [59] explored blockchain-based federated learning to secure healthcare 5.0 data. The blockchain, combined with deep extreme learning machines, determines energy consumption gauges which analyse data in real-time. The application of blockchain achieves an accuracy of 93.22% for Parkinson's disease prediction and obtains 96.18% accuracy for the estimation of intrusion detection in the healthcare 5.0 system.

The contemporary approaches, descriptions, weaknesses, and strengths of cyber threats in mHealth are presented in Table 5.

Table 5 Contemporary approaches, descriptions, weaknesses, and strengths

Contemporary approaches	Description	Weakness	Strength	Reference
Artificial Intelligence/Machine Learning	This detects anomalies by establishing behavioral checks for users and interconnected devices	Involved many computational resources and training data requires high-quality	Finds unknown threats and enhances real-time detection	[24, 81, 84, 102]
Endpoint Detection and Response	Enables continuous monitoring and incident response for all connected endpoint devices	Increase battery and processing capacity, especially in mobile devices	Mostly good for decentralized mHealth systems	[20, 24, 153].
Threat Intelligence Sharing	Provide a framework for aggregating threat data from different sources to predict and combat attacks	Continuous integration with the health infrastructure is required	Provide a proactive defence mechanism against rising threats	[28, 29, 160]
Zero Trust Architecture	Implore frameworks that enforce strict authentication for users, connected devices, and apps	Have a higher initial cost for implementation and user friction	Lowers attack surfaces, especially on distributed systems.	[24, 33]
Blockchain for Data Integrity	Maintains a secure and tamper-proof data exchange among mobile health systems and network devices	The scalability feature is limited and intensive resources	Enhances high-level data integrity and associated trust	[53, 59, 154] [51, 53, 59, 154]

5.2 Centralized and decentralized detection approaches

This section discusses the centralized and decentralized approaches for cyber threat detection in mobile healthcare.

5.2.1 Centralized detection approach

This approach unifies threat detection in a centralized manner [59]. For example, a single hub, like a security operations center (SOC). Accordingly, all data produced by networks, applications, and mobile healthcare devices is sent to a central location for processing and analysis [161]. Unified oversight and coordination are made possible by this method, which facilitates monitoring various threats throughout the ecosystem, including malware infiltration, unauthorized data access, and network anomalies. By combining data, centralized systems can use cutting-edge technology like machine learning for threat prediction and real-time analytics to identify and address possible threats. Additionally, centralization makes it easier to apply security standards and compliance measures consistently, guaranteeing that private health data complies with laws like the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability (HIPAA) [162, 163].

However, in the context of mHealth, centralized systems have significant drawbacks. Mobile health devices frequently function in dynamic, dispersed settings, including remote locations or use cases involving people who are always on the go, where there may be spotty or restricted connectivity to the central system. Endpoints may become vulnerable because of delayed threat detection and response. Furthermore, centralized systems create a single point of failure, making the entire mHealth network vulnerable if the central hub is compromised [164]Sensitive health information is sent to and stored in a single location, raising privacy issues and the possibility of security breaches. Even though centralized detection offers strong analytical skills and centralized management, it may need to be combined with decentralized or hybrid models to handle the difficulties of mobile healthcare settings.

Table 6 Comparative analysis of centralised and decentralised detection

Feature	Centralised detection	Decentralised detection
Response time	Central processing makes it slower	Faster because of local processing
Resilience	Susceptible to central failures	It is highly resilient
Best use case	Small to medium systems	Large, distributed system
Scalability	It is moderate	It is high
Cost	Lower	Higher
Management	Easy with policy enforcement	Complex to manage and synchronise
Data privacy	Higher risk with aggregated data	Privacy enhancement with local data handling
Analytic methods	Machine learning-based anomaly detection, signature-based detection, behavioural analytics, and big data analytics.	Edge computing analytics, rule-based systems, blockchain-based security, and federated learning

5.2.2 Decentralized detection approach

It involves monitoring and response capabilities across distinct network nodes or devices instead of combining them into a single system. With this method, wearables, smartphones, and Internet of Things-enabled medical equipment may process and evaluate data locally for any vulnerabilities [147, 165]. When communication to a central server is restricted, decentralised solutions can offer faster threat identification and response by identifying anomalies and malicious activity at the source. For instance, a mHealth device can independently start mitigation actions after locally detecting anomalous data patterns or illegal access. Due to eliminating dependency on a single central location, this localised processing improves robustness and lowers latency.

Decentralised methods, however, have drawbacks of their own. To analyse threats, each device needs to have enough processing power and resources, which may not be possible for all mHealth devices because of hardware constraints [63, 166]. Furthermore, it might be difficult to coordinate and manage threat intelligence across many dispersed endpoints [167], which could result in uneven security coverage. These systems may also lack a unified perspective of the network in the absence of central oversight, which makes it more difficult to identify coordinated or multi-vector attacks. Notwithstanding these drawbacks, decentralised detection offers significant benefits in dynamic mHealth settings where low latency, scalability, and robustness are essential. Organisations can successfully protect sensitive health data and infrastructure by combining decentralised systems and centralised analysis in a hybrid model, which capitalises on the advantages of both strategies.

The comparative analysis of centralised and decentralised detection based on their feature is presented in Table 6.

6 Discussion and findings

This extensively discusses various studies on mobile healthcare systems and cyber threats in mobile healthcare applications published from 2018 to 2025. Precisely, the study is divided into 8 sections. These include introduction, methodology, mobile healthcare systems, cyber threats in mobile healthcare applications, cyber threat detection approaches in mHealth, discussion, future research direction, and conclusion. Furthermore, through the research questions (RQ) formulated in Sect. 2.1, we addressed the study areas based on our findings from the 40 primary papers screened in Sect. 2 (methodology).

6.1 RQ1: how has the evolution of mobile healthcare systems impacted the delivery of personalized healthcare services over the past decade?

The findings of this intensive review indicated that out of 40 primary papers, only 7 papers ([1, 6, 13, 26, 44, 50, 59]) were utilized to discuss the evolution of mobile healthcare systems. Our findings showed that the trend of mobile healthcare systems has become increasingly a reality. These trends include early telemedicine experiments (1960–1980 s), growth of mobile telephony (1990s), the rise of smartphones and mobile health apps (2000s), wearable health technology and integration with IoT (2010s), and AI-enhanced mobile health, remote patient monitoring (2020s-present), and emerging technologies and future directions. The evolution of the mHealth advancement is highlighted in Sect. 3.1. The deployment and adoption of mobile-based healthcare services made it easy for every household and healthcare provider to interact with them daily. We further contribute the trends, features, and descriptions of mHealth for knowledge optimization.

6.2 RQ2: what are the main technologies driving the growth of mobile healthcare systems, and how do they enable improved patient care and monitoring?

The findings of this in-depth review section revealed that 20 out of 40 primary papers discussed the main technologies driving mHealth adoption and how it is improving patient care and monitoring in the healthcare industry. These studies include [52–56, 59, 61, 63–67, 70–73, 76, 78, 100] Also, our findings showed that the main technologies are broken into four key areas, namely, wireless communication [52, 54–56], the Internet of Things (IoT), and the Internet of Medical Things (IoMT) [58, 61, 63, 65, 66], data analytics, and AI [3, 67, 70–72, 100], and cloud computing [76, 78]. The main technologies that drive the growth of mHealth systems are discussed in Sect. 3.2. The findings further showed descriptions, challenges, strengths, and application areas of the main technologies as presented in Table 3 utilized in such perspectives.

6.3 RQ3: how does the growing adoption of mobile healthcare applications impact the security challenges associated with their use?

However, from the extensive review, we discovered that 5 out of 40 primary materials [21, 23, 25, 100, 102], highlighted peculiar cyber threats challenging the adoption of mobile healthcare applications in healthcare settings as presented in Sect. 4.1. The findings identified 8 common cyber threats posed as a security challenge in mHealth service delivery due to the sensitive nature of data within the healthcare environment. Therefore, these common threats include DoS/DDoS [21], Crackers, Phishing [102], Hacker's vulnerability exploitation, Malware [23, 100], Ransomware [104], Data Breaches [25], and Insecure APIs, which are presented in Sect. 4.1.1. The findings further revealed cyber threats as grouped into key categories based on their operational methods and the spproaches used by the attackers. These include data compromise, malicious attacks, insecure systems, and user vulnerabilities as explained in Sect. 4.1.2. The categories, descriptions, causes, and impacts of cyber threats for mHealth settings are presented in Table 5.

6.4 RQ4: what mitigation strategies have been proposed or implemented to address cyber threats in mobile healthcare applications?

Nevertheless, during the critical review, we identified 6 out of the 40 primary studies [26, 63, 118, 143, 145, 168],, which discussed the mitigation strategies or solutions towards addressing the inherent security challenges faced with the implementation of mHealth. We identified 5 mitigation strategies, namely, robust security practice [26, 118], user education, regular vulnerability assessments [168], compliance with regulatory standards, and adoption of advanced cybersecurity technology [63, 143, 145, 168]. These are explained in Sect. 4.2.

6.5 RQ5: what are the cyber threats that are most prevalent in mobile healthcare applications, and what vulnerabilities do they exploit?

The findings of this extensive review showed that 26 out of 40 primary published papers examined the cyber threats in mobile healthcare applications and their vulnerabilities. The study papers include [25, 29, 31, 33, 53, 56, 63, 66, 81, 82, 84, 85, 87, 88, 102, 118, 143, 147, 148, 152, 155, 161, 164, 165, 168]. The further findings in the study showed that cyber threats in mHealth apps are categorized into 2 approaches, traditional and contemporary approaches in cyber threat detection in the mHealth environment [29, 53, 59, 81, 84, 102, 118, 143] as discussed in Sect. 5.1, and the centralized and decentralized detection approach [59, 63, 147, 164, 165] as highlighted in Sect. 5.2. The contemporary approaches, descriptions, weaknesses, and strengths of cyber threats in mHealth are presented in Table 4, whereas the comparative analysis of centralized and decentralized detection based on their feature is presented in Table 5.

6.6 RQ6: which future research direction is the researcher's concentration on cyber threats in mHealth applications?

In addition to an extensive research review, there are future research focuses identified by the researchers in cyber threats for mHealth applications adoption, implementation, and deployment. The specific open research directions include AI-based threat detection [81, 154] Federated learning [44, 60, 169] Blockchain technology [118, 165], 5G and IoT advancements [32, 118, 170, 171], Better integration with heterogeneous data [33, 45, 76, 170, 172, 173] and Quantum computing or advanced encryption methods [174, 175] as highlighted in Sect. 8.

7 Future research directions

Six (6) auspicious future research areas were identified during this review. These are briefly discussed to guide scholars on the proliferation of gaps that need to be filled to further improve mitigation strategies in addressing the peculiar challenges facing the effective implementation of mobile healthcare applications during and after technology integration.

(i) AI-based threat detection: Future research in AI-based threat detection for mHealth should focus on building improved algorithms to identify complex and dynamic cybersecurity threats in real-time. Current AI systems frequently rely on previous data to predict attacks, which may not account for unique attack pathways. Adaptive AI models that use unsupervised learning to identify hitherto unidentified irregularities in mHealth systems should be investigated in research [154]. Furthermore, research

might investigate the privacy and ethical ramifications of applying AI in delicate healthcare settings, making sure that these systems improve security without unintentionally compromising user data [74, 81]. Combining AI with additional security tools like behavioral analytics and intrusion detection systems (IDS) is another exciting approach [59]. To give more precise threat identification, the research could examine how AI can examine trends in user behavior and network activities. To customize AI solutions to the difficulties of mHealth apps, such as safeguarding private patient data while preserving system efficiency and usability, cooperation between cybersecurity specialists and medical professionals is crucial.

(ii) Federated learning: By allowing decentralized data training without sending private patient data to a central server, federated learning presents a novel way to secure machine learning in mHealth. Future studies should examine how federated learning might preserve the accuracy of AI models while improving privacy and security [176] in mHealth applications [44, 168]. Research might also investigate ways to lessen possible weaknesses like poisoning assaults, in which malevolent actors alter local data to undermine the model. Research on federated learning should also focus on efficiency and scalability in situations with restricted resources, including mobile devices with little processing power [60]. Federated learning might be more feasible for broad use in mHealth if lightweight techniques are investigated and node-to-node connectivity is improved [177]. These developments could provide strong AI-driven insights across distributed systems while protecting sensitive health data.

(iii) Blockchain technology: Blockchain technology has a lot of potential to improve the security and integrity of data in mHealth applications. Developing scalable blockchain frameworks that are suited to the unique requirements of mHealth, like the safe and unchangeable storage of electronic health records (EHRs), may be the focus of future research [165]. Research should also investigate how blockchain might help stakeholders share data securely, guaranteeing that only those with permission can access private data while preserving auditability and transparency. Integrating blockchain with cutting-edge technologies like AI and IoT in mHealth is another important area for research [51, 118]. The potential for smart contracts—self-executing agreements on the blockchain—to automate adherence to legal requirements like GDPR and HIPAA could be the subject of future research. To make the technology workable for real-time mHealth applications, however, issues like high energy consumption and latency in blockchain networks must also be resolved.

(iv) 5G and IoT advancements: mHealth security faces new opportunities and difficulties as 5G networks and IoT devices proliferate in the healthcare industry. Future studies should examine how the high-speed, low-latency capabilities of 5G can improve the security of data transfer and real-time health monitoring [32, 170]. Research might focus on possible weaknesses brought about by IoT devices, such as shoddy authentication procedures and unsafe firmware, which could act as entry sites for cyberattacks. In addition, in mHealth, research is concentrated on creating strong frameworks for protecting the networked ecosystem of IoT devices [118, 171, 178]. This entails looking into techniques for dynamic access control, data stream encryption, and secure device onboarding. Security must be given top priority during the integration of 5G and IoT in mHealth to guarantee that these technologies improve patient safety and data privacy rather than endanger them.

(v) Better integration with heterogeneous data: Achieving safe and smooth integration is made more difficult by the increasing variety of data sources in mHealth, such as wearable technology, electronic health records, and patient-reported outcomes. To safely aggregate and analyze diverse data while protecting data privacy, future research will concentrate on creating standardized protocols and frameworks. To guarantee that data from various sources may be accessed and processed without disclosing sensitive information, this involves investigating cutting-edge encryption methods and secure APIs [45, 76]. Another area of attention is the application of AI and machine learning to manage and analyze heterogeneous data in real-time [33, 170, 179]. Research could study how safe federated learning models can be utilized to process various datasets without compromising privacy [172, 173]. These developments would protect patient data while allowing mHealth apps to provide more accurate and individualized healthcare insights. Also, the integration of industrial control systems and IoT enhances communication and collaborative mechanisms within interconnected systems [180]. This will ensure the identification and mitigation of deceptive connectivity disruptions across the devices on the network.

(vi) Quantum computing or advanced encryption methods: To protect mHealth applications from future quantum threats, future research should focus on developing post-quantum cryptographic algorithms that are efficient enough to run on resource-constrained devices commonly used in mHealth [174, 175]. Quantum computing presents both opportunities and threats to mHealth cybersecurity. While quantum algorithms have the potential to break current encryption standards, they also offer the potential to develop quantum-resistant encryption methods. Additionally, by enabling ultra-secure communication techniques like quantum key distribution (QKD) and attribute-based anti-quantum public-key encryption scheme (AQPKES), studies might examine how quantum computing can improve data security in mHealth [175, 181]. The practical difficulties of incorporating quantum technologies into the current mHealth infrastructure should also be covered in studies to guarantee a smooth and economical transition to quantum-resistant systems. These advancements will be critical for maintaining the long-term security of mHealth applications in the face of evolving technological landscapes.

8 Conclusion

In this systematic review, we provided significant, detailed studies on cyber threats in mobile healthcare (mHealth) applications that have been published currently, especially from 2018 to 2025 with 40 primary studies reviewed. Mobile healthcare services have revolutionized the healthcare industry. However, the cybersecurity threats dealing with mHealth systems also increase as their use increases. The continuous rise of cybersecurity threat activity has speedily affected the healthcare delivery sector recently. Even though the traditional cyber threat approaches remain the key, our study highlights the contemporary approach and mitigation strategies to detect the evolving cyber threats peculiar to mHealth utilization. This paper emphasizes the need for decentralized cyber threat detection, privacy preservation, and advanced detection techniques such as artificial intelligence (AI) integration, blockchain technology, and federated learning. These offer real benefits for both early detection, protection, and safeguards of substantial devices on networks,

and safe financial costs before they lead to more critical cyber incidents. Despite the contributions of mobile healthcare systems and cybersecurity in protecting digital tools and network devices in space, numerous threats persist. Our systematic review includes data compromise, malicious attacks, insecure systems, and user vulnerabilities. Moreover, the urgent need for cybersecurity experts and adherence to cybersecurity methodologies, standard healthcare regulations, and ethics remains a serious concern. Addressing these gaps is important for moving towards cyber threat mitigation strategies, continuing to emphasize the innovative ideas in cyber threat approaches to ameliorate the inherent cyber threat ravaging mobile healthcare settings.

Our systematic review further highlights strong adherence to these mitigation strategies as a way of tackling the inherent issues experienced in mHealth apps. The findings include full leverage of robust security practices, user education, regular vulnerability assessments, compliance with regulatory standards, and adoption of advanced cybersecurity technology. From the findings, we provided open research directions such as integration of AI-based threat detection, implementation of federated learning (FL) and blockchain technology, 5G and IoT advancements, integration of heterogeneous data and quantum computing, or advanced encryption methods. These will improve the security and privacy of health-sensitive data against cyberattacks in the digital space. The practical implication of this study will offer all health use cases, such as patients, health professionals and workers, health delivery agencies, government at all levels, health developers and promoters, health industry 5.0, and researchers to improve the security and privacy of healthcare heterogeneous data.

Author contributions
ACI ontributed right from the conceptualization and design, materials sourcing, manuscript preparation, graphic and table preparation including the first draft of the structure and writing. Manuscript editing and grammatical checks were performed by URA. HFN participated in drafting the structure and proofreading the manuscript. Also, all the authors read and approved the final manuscript.

Funding
There is no external funding received by the authors.

Data availability
No datasets were generated or analysed during the current study.

Declarations

Ethics approval and consent to publication
This article does not contain any studies with human participants performed by the authors.

Consent to participate
Not applicable.

Competing interests
The authors declare no competing interests.

Clinical trial number
Not applicable.

Received: 14 February 2025 / Accepted: 14 July 2025
Published online: 17 July 2025

References

1. Istepanian RSH. Mobile health (m-Health) in retrospect: the known unknowns. Int J Environ Res Public Health. 2022. https://doi.org/10.3390/ijerph19073747.

2. Simple C, Telehealth vs Telemedicine vs mHealth, and, How RPMF. In, CareSimple Inc. Accessed: Feb. 10, 2025. [Online]. Available: https://caresimple.com/telehealth-vs-telemedicine-vs-mhealth-and-how-rpm-fits-in/
3. Moshawrab M, Adda M, Bouzouane A, Ibrahim H, Raad A. Reviewing federated machine learning and its use in diseases prediction. Sensors. 2023;23(4):1–39. https://doi.org/10.3390/s23042112.
4. Anikwe CV et al. Mobile and wearable devices for health monitoring: review of sensors, components modules, applications and future prospects. Expert Syst Appl. 117362, 2022.
5. Thanh H, et al. Agriculture 4. 0 and beyond: evaluating cyber threat intelligence sources and techniques in smart farming ecosystems. Comput Secur. 2024;140:103754. https://doi.org/10.1016/j.cose.2024.103754.
6. Fereidooni H, Dmitrienko A, Rieger P, Miettinen M, Sadeghi AR, Madlener F. FedCRI: Federated Mobile Cyber-Risk Intelligence, *29th Annual Network and Distributed System Security Symposium, NDSS 2022*, no. April, 2022, https://doi.org/10.14722/ndss.2022.23153
7. Pappas G, Walther T, Mattila S, Denis T, Brock G. Cybersecurity Nightmares: The Cost of Healthcare Cyberattacks in 2024, Intraprisehealth. [Online]. Available: https://intraprisehealth.com/the-cost-of-cyberattacks-in-healthcare/
8. Southwick R. The 10 largest health data breaches of the first half of 2024, 2024.
9. Sunnyvale C, Third Annual Ponemon Institute Report. Nearly Seven in 10 Healthcare Organizations Experienced Disruption to Patient Care Due to Cyber Attacks,: 2024.
10. Dall E. Healthcare Industry Biggest Attacks (2023– 2024), 2024.
11. Bruce G. Hospital cyberattack costs, patient care disruptions up: 9 things to know, 2023.
12. Joel W, Healthcare Cyber Attack Statistics. 2022: 25 Alarming Data Breaches You Should Know, Expert Insights. Accessed: Oct. 20, 2024. [Online]. Available: https://expertinsights.com/insights/healthcare-cyber-attack-statistics/
13. González Bermúdez A, Carramiñana D, Bernardos AM, Bergesio L, Besada JA. A fusion architecture to deliver multipurpose mobile health services. Comput Biol Med. 2024;173. https://doi.org/10.1016/j.compbiomed.2024.108344.
14. Ghayoomi H, Laskey K, Miller-Hooks E, Hooks C, Tariverdi M. Assessing resilience of hospitals to cyberattack. Digit Health. 2021;7. https://doi.org/10.1177/20552076211059366.
15. Kumar M, Yadav V, Yadav SP. Advance comprehensive analysis for zigbee network-based IoT system security. Discover Computing. 2024. https://doi.org/10.1007/s10791-024-09456-3.
16. Tariq N, et al. The security of big data in fog-enabled Iot applications including blockchain: A survey. Sens (Switzerland). 2019;19(8):1–33. https://doi.org/10.3390/s19081788.
17. Meyers A, Shirk B, Zaitsev E, Etheridge T. 2023 Global Threat Report: From Relentless Adversaries to Resilient Businesses, 2024.
18. Lau J. State of Cybersecurity 2023: Navigating Current and Emerging Threats, 2023.
19. Sullivan B. The 2024 Study on Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care, 2024.
20. Balantrapu SS. Current trends and future directions exploring machine learning techniques for cyber threat detection. Int J Sustainable Dev Through AI. 2024;3(2):1–15. ML and IoT.
21. Wang T, et al. Federated Learning-based information leakage risk detection for secure medical internet of things. ACM Trans Internet Technol. 2024;1–21. https://doi.org/10.1145/3639466.
22. Kumar A, Mozar S. Lecture Notes in Electrical Engineering, in *ICCCE: International Conference on Communications and Cyber Physical Engineering* 2018, Singapore: Springer Nature Singapore Pte Ltd, 2019, pp. 1–775. https://doi.org/10.1007/978-981-13-0212-1
23. Alo UR, Nweke HF, Ele SI. Machine learning-based framework for automatic malware detection using Android traffic data. J Theor Appl Inf Technol. 2021;99(15):3782–800.
24. Ofoegbu KD, Osundare OS, Ike CS, Fakeyede OG, Ige AB. Real-Time cybersecurity threat detection using machine learning and big data analytics: A comprehensive approach. Comput Sci IT Res J. 2023;4(3):478–501. https://doi.org/10.51594/csitrj.v4i3.1500.
25. Duary S, Choudhury P, Mishra S, Sharma V, Rao DD, Aderemi AP. Cybersecurity Threats Detection in Intelligent Networks using Predictive Analytics Approaches, in *4th International Conference on Innovative Practices in Technology and Management 2024, ICIPTM 2024*, 2024, pp. 1–6. https://doi.org/10.1109/ICIPTM59628.2024.10563348
26. Coelho KK, Tristão ET, Nogueira M, Vieira AB, Nacif JAM. Multimodal biometric authentication method by federated learning. Biomed Signal Process Control. 2023. https://doi.org/10.1016/j.bspc.2023.105022.
27. Weichbroth P, Łysik Ł. Mobile security: threats and best practices. Mob Inform Syst. 2020;2020. https://doi.org/10.1155/2020/8828078.
28. Sakib SMN. Cyber threat intelligence. Cyber Threat Intell. 2022;1–276. https://doi.org/10.1002/9781119861775.
29. Arazzi M et al. NLP-Based Techniques for Cyber Threat Intelligence, *arXiv:2311.08807v1 [cs.CR]*, pp. 1–63, 2023.
30. Alenoghena CO, et al. eHealth: a survey of architectures, developments in mHealth, security concerns and solutions. Int J Environ Res Public Health. 2022. https://doi.org/10.3390/ijerph192013071.
31. Cartwright AJ. The elephant in the room: cybersecurity in healthcare. J Clin Monit Comput. 2023;37(5):1123–32. https://doi.org/10.1007/s10877-023-01013-5.
32. Aldhaheri A, Alwahedi F, Ferrag MA, Battah A. Deep learning for cyber threat detection in IoT networks: a review. Internet Things Cyber-Physical Syst. 2024;4:110–28. https://doi.org/10.1016/j.iotcps.2023.09.003.
33. Mahboubi A, et al. Evolving techniques in cyber threat hunting: A systematic review. J Netw Comput Appl. 2024;232:104004. https://doi.org/10.1016/j.jnca.2024.104004.
34. ElSayed Z, Abdelgawad A, Elsayed N. Cybersecurity and Frequent Cyber Attacks on IoT Devices in Healthcare: Issues and Solutions, *arXiv preprint arXiv:2501.11250.*, 2025, [Online]. Available: http://arxiv.org/abs/2501.11250
35. Randles R, Finnegan A. Guidelines for writing a systematic review. Nurse Educ Today. 2023;125: 105803. https://doi.org/10.1016/j.nedt.2023.105803.
36. Carrera-Rivera A, Ochoa W, Larrinaga F, Lasa G. How-to conduct a systematic literature review: A quick guide for computer science research. MethodsX. 2022;9:101895. https://doi.org/10.1016/j.mex.2022.101895.
37. Fitzpatrick L. The Future of Healthcare Is Mobile, 2021.
38. Cousineau C. Healthcare's Evolution: Important Healthcare Trends in 2024, 2024.
39. Bocas J. Emerging Mobile Health Trends in 2024, 2023.
40. Martinez A. Mobile Health Apps: How Are They Reshaping Healthcare in 2024, 2024.

41. Hu J, Jiang H, Xiao Z, Chen S, Dustdar S, Liu J. HeadTrack: Real-Time Human–Computer interaction via wireless earphones. IEEE J Sel Areas Commun. 2023;42(4):990–1002.
42. Sun, Gang Y, Li D, Liao, Victor, Chang. Service function chain orchestration across multiple domains: A full mesh aggregation approach. IEEE Trans Netw Serv Manage. 2018;15(3):1175–91.
43. Sun G, Liao D, Zhao D, Xu Z. Live migration for multiple correlated virtual machines in cloud-based data centers. IEEE Trans Serv Comput. 2015;11(2):279–91.
44. Shivhare I, Jogani V, Purohit J, Shrawne SC. Analysis of Explainable Artificial Intelligence Methods on Medical Image Classification, 2023 *3rd International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies, ICAECT 2023*, 2023. https://doi.org/10.1109/ICAECT57570.2023.10118312
45. Pabalkar V, Chanda R. Role of artificial intelligence in healthcare. Cogn Sci Technol. 2023;F1493(6):353–60. https://doi.org/10.1007/978-981-99-2746-3_37. Part.
46. Rehman A, Ma H, Ozturk I, Ahmad MI. Examining the carbon emissions and climate impacts on main agricultural crops production and land use: updated evidence from Pakistan. Environ Sci Pollut Res. 2022;29(1):868–82.
47. Boiano A et al. A Secure and Trustworthy Network Architecture for Federated Learning Healthcare Applications, *arXiv:2404.11698v1 [cs.AI]*, vol. 1, no. 101080564, 2024.
48. Mazhar T, Shahzad T, Amir M, Generative AI. IoT, and blockchain in healthcare: application, issues, and solutions. Discover Internet Things. 2025;5(5). https://doi.org/10.1007/s43926-025-00095-8.
49. Rehman A, Sagheer A, Khan MA, Ghazal TM, Adnan KM, Mosavi A. A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique. Comput Biol Med. 2022;150:106019. https://doi.org/10.1016/j.compbiomed.2022.106019.
50. Alhomsi Y, Alsalemi A, Al Disi M, Bensaali F, Amira A, Alinier G. CouchDB based Real-Time wireless communication system for clinical simulation. Proc– 20th Int Conf High Perform Comput Commun 16th Int Conf Smart City 4th Int Conf Data Sci Syst HPCC/SmartCity/DSS 2018. 2019;1094–8. https://doi.org/10.1109/HPCC/SmartCity/DSS.2018.00182.
51. Kang J, Xiong Z, Niyato D, Zou Y, Zhang Y, Guizani M. Reliable federated learning for mobile networks. IEEE Wirel Commun. 2020;27(2):72–80. https://doi.org/10.1109/MWC.001.1900119.
52. Leith DJ, Farrell S. Coronavirus Contact Tracing: Evaluating The Potential Of Using Bluetooth Received Signal Strength For Proximity Detection, *scss.tcd.ie*, pp. 1–11, 2020.
53. Greenberg-Worisek AJ, Kurani S, Finney Rutten LJ, Blake KD, Moser RP, Hesse BW. Tracking healthy people 2020 internet, broadband, and mobile device access goals: an update using data from the health information National trends survey. J Med Internet Res. 2019;21(6):1–11. https://doi.org/10.2196/13300.
54. Subasi A, Bandic L, Qaisar SM. Cloud-based health monitoring framework using smart sensors and smartphone. Elsevier Inc.; 2020. https://doi.org/10.1016/B978-0-12-819043-2.00009-5.
55. El-deep SE, Abohany AA, Sallam KM, El-Mageed AAA. A comprehensive survey on impact of applying various technologies on the internet of medical things. Artif Intell Rev. 2025. https://doi.org/10.1007/s10462-024-11063-z.
56. Nguyen DC, et al. Federated learning for smart healthcare: A survey. ACM Comput Surv. 2022;55(3):1–35. https://doi.org/10.1145/3501296.
57. Ma Q, Zhang Y, Zhou FHH, Hao H. Nip it in the bud: the impact of china's large-scale free physical examination program on health care expenditures for elderly people. Humanit Social Sci Commun. 2025;12(1):1–16.
58. Sachin DN, Annappa B, Hegde S, Abhijit CS, Ambesange S. FedCure: A Heterogeneity-Aware personalized federated learning framework for intelligent healthcare applications in IoMT environments. IEEE Access. 2024;12:15867–83. https://doi.org/10.1109/ACCESS.2024.3357514.
59. Haoyu L, Jianxing L, Arunkumar N, Hussein AF, Jaber M. An IoMT cloud-based real time sleep apnea detection scheme by using the SpO2 estimation supported by heart rate variability. Future Gener Comput Syst. 2018;98:69–77.
60. Zhang L, Wu Y, Chen L, Fan L, Nallanathan A. Scoring aided federated learning on Long-Tailed data for wireless IoMT based healthcare system. IEEE J Biomed Health Inf. 2024;28(6):3341–8. https://doi.org/10.1109/JBHI.2023.3300173.
61. Aminifar A, Shokri M, Aminifar A. Privacy-preserving edge federated learning for intelligent mobile-health systems. Future Gener Comput Syst. 2024;161:625–37. https://doi.org/10.1016/j.future.2024.07.035.
62. Hu F, Yang H, Qiu L, Wei S, Hao Hu, and, Zhou H. Spatial structure and organization of the medical device industry urban network in china: evidence from specialized, refined, distinctive, and innovative firms. Front Public Health. 2025;13:1518327.
63. Anikwe CV, et al. Mobile and wearable sensors for data-driven health monitoring system: State-of-the-art and future prospect. Expert Syst Appl. Sep. 2022;202:117362. https://doi.org/10.1016/j.eswa.2022.117362.
64. Vekaria D, Kumari A, Tanwar S, Kumar N. ξ boost: an AI-based data analytics scheme for COVID-19 prediction and economy boosting. Internet Things J. 2021;1–12. https://doi.org/10.1109/JIOT.2020.3047539.
65. Shokr A, et al. Mobile health (mHealth) viral diagnostics enabled with adaptive adversarial learning. ACS Nano. 2022;15(1):665–73. https://doi.org/10.1021/acsnano.0c06807.
66. Moshawrab M, Adda M, Bouzouane A, Ibrahim H, Raad A. Cardiovascular Events Prediction using Artificial Intelligence Models and Heart Rate Variability, *Procedia Comput Sci*, vol. 203, no. 2019, pp. 231–238, 2022. https://doi.org/10.1016/j.procs.2022.07.030
67. Dayakaran D, Kadiresan N. Federated Learning Framework for Human Activity Recognition Using Smartphones, *Procedia Comput Sci*, vol. 235, no. 2023, pp. 2069–2078, 2024. https://doi.org/10.1016/j.procs.2024.04.196
68. Nweke H, Ikegwu AC, Nwafor CA, Ogbaga IN. Smartphone-based human activity recognition using Artificial Intelligence Methods and Orientation Invariant Features, *Nigeria Computer Society: International Conference on Technological Solutions for Smart Economy, SmartEco2024*, vol. 35, pp. 1–8, 2024.
69. Khamaj A. Ai-enhanced chatbot for improving healthcare usability and accessibility for older adults. Alexandria Eng J. 2025;116:202–13. https://doi.org/10.1016/j.aej.2024.12.090.
70. Wu Q, Chen X, Zhou Z, Zhang J. Fedhome: cloud-edge based personalized federated learning for in-home health monitoring. IEEE Trans Mob Comput. 2022;21(8):2818–32. https://doi.org/10.1109/TMC.2020.3045266.
71. Verma A, Agarwal G, Gupta AK, Sain M. Novel hybrid intelligent secure cloud internet of things based disease prediction and diagnosis. Electronics. 2021. https://doi.org/10.3390/electronics10233013.

72. Stergiou C, Psannis KE, Kim B, Gupta B. Secure Integration of Internet-of-Things and Cloud Computing Secure integration of IoT and Cloud Computing, *Future Generation Computer Systems*, vol. 78, no. December, pp. 964–975, 2016, https://doi.org/10.1016/j.future.2016.11.031
73. Kumar PM, Lokesh S, Varatharajan R, Chandra Babu G, Parthasarathy P. Cloud and IoT based disease prediction and diagnosis system for healthcare using fuzzy neural classifier. Future Gener Comput Syst. 2018;86:527–34. https://doi.org/10.1016/j.future.2018.04.036.
74. Ishikiriyama CS, Francisco C, Gomes S. Big data: a global overview. Cham: Springer; 2019. https://doi.org/10.1007/978-3-319-93061-9.
75. Alars ESA, Kurnaz S. Enhancing network intrusion detection systems with combined network and host traffic features using deep learning: deep learning and IoT perspective. Discover Comput. 2024;27(1). https://doi.org/10.1007/s10791-024-09480-3.
76. Labu MR, Ahammed MF. Next-Generation cyber threat detection and mitigation strategies: A focus on artificial intelligence and machine learning. J Comput Sci Technol Stud. 2024;6(1):179–88. https://doi.org/10.32996/jcsts.2024.6.1.19.
77. Dey AK, Gupta GP, Sahu SP. A metaheuristic-based ensemble feature selection framework for cyber threat detection in IoT-enabled networks. Decis Anal J. 2023;7: 100206. https://doi.org/10.1016/j.dajour.2023.100206.
78. Lee J, Kim J, Kim I, Han K. Cyber threat detection based on artificial neural networks using event profiles. IEEE Access. 2019;7:165607–26. https://doi.org/10.1109/ACCESS.2019.2953095.
79. Ullah F, Ullah S, Naeem MR, Mostarda L, Rho S, Cheng X. Cyber-threat detection system using a hybrid approach of transfer learning and multi-model image representation. Sensors. 2022. https://doi.org/10.3390/s22155883.
80. Sun N, et al. Cyber threat intelligence mining for proactive cybersecurity defense: A survey and new perspectives. IEEE Commun Surv Tutorials. 2023;25(3):1748–74. https://doi.org/10.1109/COMST.2023.3273282.
81. Ferrag MA, et al. Revolutionizing cyber threat detection with large Language models: A Privacy-Preserving BERT-Based lightweight model for iot/iiot devices. IEEE Access. 2024;12:23733–50. https://doi.org/10.1109/ACCESS.2024.3363469.
82. Narmadha K, Varalakshmi P. Federated learning in healthcare: A privacy preserving approach. Stud Health Technol Inf. 2022;294:194–8. https://doi.org/10.3233/SHTI220436.
83. Sun G, Xu Z, Yu H, Chang V. Dynamic network function provisioning to enable network in box for industrial applications. IEEE Trans Ind Inf. 2021;17(10):7155–64. https://doi.org/10.1109/TII.2020.3042872.
84. Papakostas G, Shakya S, Kamel AK. Mobile Computing and Sustainable Informatics, in *Proceedings of ICMCSI 2023*, 2023. https://doi.org/10.1007/978-981-99-0835-6
85. Lorenzini G, Shaw DM, Elger BS. It takes a pirate to know one: ethical hackers for healthcare cybersecurity. BMC Med Ethics. 2022;23(1):1–8. https://doi.org/10.1186/s12910-022-00872-y.
86. Shavazipour A, Jan H, Multi-scenario K, Shavazipour B, Kwakkel JH, Miettinen K. *Cyber security in healthcare systems*, vol. 144, no. 2. 2021.
87. Zarrin J. Blockchain for decentralization of internet: prospects, trends, and challenges. Cluster Comput, 8, 2021.
88. Kissi J, et al. Healthcare professionals' perception on emergence of security threat using digital health technologies in healthcare delivery. Digit Health. 2024;10. https://doi.org/10.1177/20552076241260385.
89. Abad G, Picek S, Ramírez-Durán VJ, Urbieta A. On the Security & Privacy in Federated Learning, *arXiv:2112.05423v2 [cs.CR]*, 2022.
90. Krishna TBM, Praveen SP, Ahmed S, Srinivasu PN. Software-driven secure framework for mobile healthcare applications in IoMT. Intell Decis Technol. 2023;17(2):377–93. https://doi.org/10.3233/IDT-220132.
91. Elsadig MA. Detection of Denial-of-Service attack in wireless sensor networks: A lightweight machine learning approach. IEEE Access. 2023;11:83537–52. https://doi.org/10.1109/ACCESS.2023.3303113.
92. Kharb L, Chahal D. ICICCT 2017, in *Proceedings of International Conference on: Information, Communication and Computing Technology*, New Delhi, India: Edupedia Publications Pvt Ltd, New Delhi, 2017, pp. 1–191. https://doi.org/10.1007/978-981-10-2750-5
93. CP B. Analysis of white and black hat hacker roles, practices and techniques, considering ethical and legal issues, including bug bounty programs. SunText Rev Econ Bus. 2023;04(04). https://doi.org/10.51737/2766-4775.2023.095.
94. Araque ED. Active cyber defense in the healthcare sector. Clark University; 2023.
95. Mathew DE, Ebem DU, Chukwu A, Pamela I, Ukeoma E, Dibiaezue NF. Recent emerging techniques in explainable artificial intelligence to enhance the interpretable and Understanding of AI models for human. Volume 123. Springer US; 2025. https://doi.org/10.1007/s11063-025-11732-2.
96. Shaukat K, Luo S, Chen S, Liu D. Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective, in *1st Annual International Conference on Cyber Warfare and Security, ICCWS 2020 - Proceedings*, 2020, pp. 1–15. https://doi.org/10.1109/ICCWS48432.2020.9292388
97. Yeng PK, Fauzi MA, Yang B, Nimbe P. Investigation into phishing risk behaviour among healthcare staff. Inform (Switzerland). 2022;13(8):1–30. https://doi.org/10.3390/info13080392.
98. Dafoe J, Chen N, Chen B, Wang Z. Enabling per-file data recovery from ransomware attacks via file system forensics and flash translation layer data extraction. Cybersecurity. 2024;7(1): 75. https://doi.org/10.1186/s42400-024-00287-9.
99. Dameff C, et al. Ransomware attack associated with disruptions at adjacent emergency departments in the US. JAMA Netw Open. 2023;6(5):e2312270. https://doi.org/10.1001/jamanetworkopen.2023.12270.
100. Neprash HT, et al. Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016–2021. JAMA Health Forum. 2022. https://doi.org/10.1001/jamahealthforum.2022.4873.
101. Bob S. The Cost of Data Breaches in Mobile Healthcare, Ponemon Institute. [Online]. Available: https://www.proofpoint.com/us/cyber-insecurity-in-healthcare
102. Aspach K. 10 Major Cyberattacks And Data Breaches In 2024 (So Far), vol. 2024, 2024.
103. Almulihi AH, Alassery F, Khan AI, Shukla S, Gupta BK, Kumar R. Analyzing the implications of healthcare data breaches through computational technique. Intell Autom Soft Comput. 2022;32(3):1763–79. https://doi.org/10.32604/IASC.2022.023460.
104. Masuch K, Greve M, Trang S. What to do after a data breach? Examining apology and compensation as response strategies for health service providers. Electron Markets. 2021;31(4):829–48. https://doi.org/10.1007/s12525-021-00490-3.
105. Khatiwada P, Fauzi MA, Yang B, Yeng P, Lin JC, Sun L. Threats and Risk on Using Digital Technologies for Remote Health Care Process, in *ACM International Conference Proceeding Series*, 2023, pp. 506–522. https://doi.org/10.1145/3626641.3627604

106. Moura P, Fazendeiro P, Inácio PRM, Vieira-Marques P, Ferreira A. Assessing access control risk for mHealth: A Delphi study to categorize security of health data and provide risk assessment for mobile apps. J Healthc Eng. 2020;2020. https://doi.org/10.1155/2020/5601068.
107. Asad M, Moustafa A, Yu C. A critical evaluation of privacy and security threats in federated learning. Sens (Switzerland). 2020;20(24):1–15. https://doi.org/10.3390/s20247182.
108. George DAS, George ASH. The emergence of cybersecurity medicine: protecting implanted devices from cyber threats. Partners Univers Innovative Res Publication. 2023;1(2):93–111. https://doi.org/10.5281/zenodo.10206563.
109. Pool J, Akhlaghpour S, Fatehi F. Towards a contextual theory of mobile health data protection (MHDP): A realist perspective. Int J Med Inf. 2020;141. https://doi.org/10.1016/j.ijmedinf.2020.104229.
110. National Institute of Standards and Technology. Mobile Device Security: Corporate-Owned Personally-Enabled (COPE), NIST Publishes SP 1800-21. [Online]. Available: https://csrc.nist.gov
111. National Institute of Standards and Technology. NIST Special Publication 800– 57: Recommendation for Key Management, 2022.
112. Rahman MA, Shamim HM, Islam MS, Alrajeh NA, Muhammad G. Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach. IEEE Access. 2020;8:205071–87. https://doi.org/10.1109/ACCESS.2020.3037474.
113. Open Web Application Security Project. OWASP Mobile Security Testing Guide, OWASP. [Online]. Available: https://owasp.org/
114. International Organization for Standardization. ISO/IEC 27001: Information Security Management, ISO. [Online]. Available: https://www.iso.org
115. Maruthupandi J, Sivakumar S, Dhevi BL, Prasanna S, Priya RK, Selvarajan S. An intelligent attention based deep convoluted learning (IADCL) model for smart healthcare security. Sci Rep. 2025;15(1):1363. https://doi.org/10.1038/s41598-024-84691-8.
116. Cybersecurity and Infrastructure Agency. Cybersecurity awareness month. Secure our World, pp. 8–10, 2024.
117. National Cyber Security Centre. Guidance for secure use of mobile applications, NCSC.
118. Federal Trade Commission. Mobile app privacy and security guidance. FTC, pp. 1–15, 2023.
119. Aljedaani B, Ahmad A, Zahedi M, Ali Babar M. Security awareness of end-users of mobile health applications: An empirical study, *ACM International Conference Proceeding Series*, pp. 125–136, 2020, https://doi.org/10.1145/3448891.3448952
120. Tadayon M, Pottie G. Predicting student performance in an educational game using a hidden Markov model. IEEE Trans Educ, pp. 1–6, 2020.
121. Wang Q, Jiang Q, Yang Y, Pan J. *The burden of travel for care and its influencing factors in China: an inpatient-based study of travel time. J Transp Health.* 2022; 25: 101353. 2022.
122. SANS Institute. Vulnerability assessment essentials for modern applications. SANSI, 2023.
123. GDPR. General Data Protection Regulation (GDPR): Guidelines for Compliance, 2022.
124. Zakes A. 2023 HIMSS Healthcare Cybersecurity Survey, 2023.
125. Klaudia B. A New Era of Healthcare: Telehealth vs. Telemedicine Explained, Healthnews. [Online]. Available: https://healthnews.com/family-health/healthy-living/telehealth-vs-telemedicine-differences/#:~:text=Telehealth isn%27t just about doctor-patient chats%3B it%27s a,diagnoses%2 C treatments%2 C and prescriptions — all delivered remotely.
126. HIPAA. HIPAA Privacy and Security Rules, 2023.
127. Koca M, Aydin MA, Sertbaş A, Zaim AH. A new distributed anomaly detection approach for log IDS management based on deep learning. Turkish J Electr Eng Comput Sci. 2021;25(9):2486–501. https://doi.org/10.3906/elk-2102-89.
128. Kostiantyn Z. Cyber Hygiene in the Context of Digital Transformation in Higher Education: Challenges and Opportunities, in *International Scientific and Practical Conference Problems of Students in Universities and New Ways of Solving them*, Paris, France: International Sceince Group, 2025. https://doi.org/10.46299/ISG.2025.1.5
129. Khanna A. Implementing effective cyber hygiene practices. Int J Adv Res Eng Technol. 2025;16(1):1–9. https://doi.org/10.34218/IJARET_16_01_001.
130. Sun X, Dai J, Liu P, Singhal A, Yen J. Using bayesian networks for probabilistic identification of Zero-Day attack paths. IEEE Trans Inf Forensics Secur. 2018;13(10):2506–21. https://doi.org/10.1109/TIFS.2018.2821095.
131. Koca M. Real-Time Security Risk Assessment From CCTV Using Hand Gesture Recognition, in *IEEE Access*, vol. 12, pp. 84548–84555, 2024, https://doi.org/10.1109/ACCESS.2024.3412930
132. Enamamu TS, Otebolaku AM, Dany J, Marchang JN. Continuous m-Health Monitoring and Patient Verification Using Bioelectrical Signals, *Preprints (Basel)*, pp. 1–18, 2020.
133. Kumar H, Sarma D, Borah S, Dutta N, Conference N. *Advances in Communication, Cloud, and Big Data*. Singapore: Springer Nature Singapore Pte Ltd., 2016.
134. Zhou W, Xia C, Wang T, Liang X, Lin W, Li X, Zhang S. Hidim: A novel framework of network intrusion detection for hierarchical dependency and class imbalance. Computers Secur. 2025;148:104155.
135. Surdjono HD, et al. Effectiveness of cybersecurity awareness program based on mobile learning to improve cyber hygiene. Int J Inf Educ Technol. 2025;15(2):220–9. https://doi.org/10.18178/ijiet.2025.15.2.2235.
136. Priyadharshini SL, et al. Unlocking cybersecurity value through advance technology and analytics from data to insight. Nanotechnol Percept. 2024;10:202–18.
137. Rabie OBJ, Selvarajan S, Hasanin T, Mohammed GB, Alshareef AM, Uddin M. A full privacy-preserving distributed batch-based certificate-less aggregate signature authentication scheme for healthcare wearable wireless medical sensor networks (HWMSNs). Int J Inf Secur. 2024;23(1):51–80. https://doi.org/10.1007/s10207-023-00748-1.
138. Li J. Attribute based signature encryption scheme based on cloud computing in medical social networks. J Cyber Secur Mobil. 2024;13(3):517–40. https://doi.org/10.13052/jcsm2245-1439.1338.
139. Bajaj S, Bopardikar SD, Torng E, Von Moll A, Casbeer DW. Multivehicle perimeter defense in conical environments. IEEE Trans Robot. 2024;40:1439–56. https://doi.org/10.1109/TRO.2024.3351556.
140. Bromiley M. 2022 SANS Protects: The Endpoint, *SANS Institute*, no. April, pp. 1–10, 2022.
141. Vegesna VV. Enhancing cyber resilience by integrating AI-Driven threat detection and mitigation strategies. Trans Latest Trends Artif Intell, 4, 4, 2023.
142. Long G, Shen T, Tan Y, Gerrard L, Clarke A, Jiang J. Federated learning for Privacy-Preserving open innovation future on digital health. Humanity Driven AI. 2022;113–33. https://doi.org/10.1007/978-3-030-72188-6_6.

143. Zhang F, et al. Recent methodological advances in federated learning for healthcare. Patterns. 2024;5(6). https://doi.org/10.1016/j.patter.2024.101006.
144. Ibrahim M, Al-Wadi A, Elhafiz R. Security analysis for smart healthcare systems. Sensors. 2024;24(11). https://doi.org/10.3390/s24113375.
145. Ahmed U, et al. Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering. Sci Rep. 2025;15(1):1726. https://doi.org/10.1038/s41598-025-85866-7.
146. Xia T, Han J, Ghosh A, Mascolo C. Cross-Device Federated Learning for Mobile Health Diagnostics: A First Study on COVID-19 Detection, in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, 2023. https://doi.org/10.1109/ICASSP49357.2023.10096427
147. Li L, Fan Y, Tse M, Lin K-Y. A review of applications in federated learning. Comput Ind Eng. 2020;149:1–2. https://doi.org/10.1016/j.cie.2020.106854.
148. Argaw ST, et al. Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks. Med Inf Decis Mak. 2020;20(1):1–10. https://doi.org/10.1186/s12911-020-01161-7.
149. Yaqoob MM, Nazir M, Khan MA, Qureshi S, Al-Rasheed A. Hybrid Classifier-Based federated learning in health service providers for cardiovascular disease prediction. Appl Sci (Switzerland). 2023;13(3). https://doi.org/10.3390/app13031911.
150. Kumar A, et al. A novel decentralized blockchain architecture for the preservation of privacy and data security against cyberattacks in healthcare. Sensors. 2022;22(15). https://doi.org/10.3390/s22155921.
151. Umoga UJ, et al. Exploring the potential of AI-driven optimization in enhancing network performance and efficiency. Magna Scientia Adv Res Reviews. 2024;10(01):368–78.
152. Bikakis N, Papastefanatos G, Skourla M, Sellis T. A hierarchical aggregation framework for efficient multilevel visual exploration and analysis. Semant Web. 2017;8(1):139–79. https://doi.org/10.3233/SW-160226.
153. Tabassum N, Ahmed M, Shorna NJ, Sowad MMUR, Haque HMZ. Depression detection through smartphone sensing: A federated learning approach. Int J Interact Mob Technol. 2023;17(1):40–56. https://doi.org/10.3991/ijim.v17i01.35131.
154. Olaoye F, Egon A. Federated learning for Privacy-Preserving security analytics. EasyChair, 2024.
155. Menon SP, et al. An intelligent diabetic patient tracking system based on machine learning for E-Health applications. Sensors. 2023;23(6):1–14. https://doi.org/10.3390/s23063004.
156. McGowan A, Sittig S, Andel T. Medical internet of things: A survey of the current threat and vulnerability landscape, in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2021, pp. 3850–3858. https://doi.org/10.24251/hicss.2021.466
157. Wang T, Du Y, Gong Y, Raymond KK, Choo, Guo Y. Applications of federated learning in mobile health: scoping review. J Med Internet Res. 2023;25:1–12. https://doi.org/10.2196/43006.
158. Garg A, Saha AK, Dutta D. Federated Neural Architecture Search, *arXiv:2002.06352v5 [cs.LG]*, vol. 5, 2022.
159. Zhang M, Wei E, Berry R, Huang J. Age-Dependent differential privacy. Perform Eval Rev. 2022;50(1):115–6. https://doi.org/10.1145/3489048.3526953.
160. İ, Avcı, Koca M. Intelligent transportation system technologies, challenges and security. Appl Sci. 2024;14(11). https://doi.org/10.3390/app14114646.
161. Ikegwu AC, Obianuju OJ, Nwokoro IS, Ofuru M, Ebem DU. Investigating the impact of AI/ML for monitoring and optimizing energy usage in smart home. Artif Intell Evol. 2025;6(1):30–43. https://doi.org/10.37256/aie.6120256065.
162. Belenguer A, Navaridas J, Pascual JA. A review of federated learning in intrusion detection systems for IoT. Comput Netw. 2025;258:111023. https://doi.org/10.1016/j.comnet.2024.111023.
163. Cheng Z et al. Kairos: practical intrusion detection and investigation using Whole-system provenance, 2024. https://doi.org/10.1109/sp54263.2024.00005
164. Alazab M, Rm SP, Parimala M, Maddikunta PKR, Gadekallu TR, Pham QV. Federated learning for cybersecurity: concepts, challenges, and future directions. IEEE Trans Industr Inf. 2022;18(5):3501–9. https://doi.org/10.1109/TII.2021.3119038.
165. Ikegwu AC, Nweke HF, Anikwe CV, Alo UR, Okonkwo OR. Tools, Challenges, Solutions and Research Directions. Cluster Comput. 2022;25(5):3343–87. https://doi.org/10.1007/s10586-022-03568-5. Big Data Analytics for Data-driven Industry: A Review of Data Sources,.
166. Islam MN, et al. Predictis: an IoT and machine learning-based system to predict risk level of cardio-vascular diseases. BMC Health Serv Res. 2023;23(1):1–25. https://doi.org/10.1186/s12913-023-09104-4.
167. Al-Garadi MA, Mohamed A, Al-Ali AK, Du X, Ali I, Guizani M. A survey of machine and deep learning methods for internet of things (IoT) security. IEEE Commun Surv Tutor. 2020;22(3):1646–85. https://doi.org/10.1109/COMST.2020.2988293.
168. Koca M, Avci I. A Novel Hybrid Model Detection of Security Vulnerabilities in Industrial Control Systems and IoT Using GCN + LSTM, *IEEE Access*, no. August, pp. 143343–143351, 2024, https://doi.org/10.1109/ACCESS.2024.3466391
169. Xu G, et al. AAQ-PEKS: an Attribute-based anti-Quantum Public-Key encryption scheme with keyword search for E-healthcare scenarios. Cryptol ePrint Arch. 2023;3:1–13.
170. Gosselin R, Vieu L, Loukil F, Benoit A. Privacy and security in federated learning: A survey. Appl Sci (Switzerland). 2022;12:1–15. https://doi.org/10.3390/app12199901.
171. Anikwe CV, Nweke HF, Alo UR, Onu UF. Mobile Based Health Monitoring System for the Elderly People using Internet of Medical Things, in *ICT4NDS2021: ICT and Sustainability in the 5th Industrial Revolution*, 2021, pp. 35–40.
172. Zhao X, Zhang Y, Yang Y. and Jay Pan. Diabetes-related avoidable hospitalisations and its relationship with primary healthcare resourcing in china: A cross-sectional study from Sichuan Province. Health Soc Care Commun 30, 4, e1143-e1156, 2022.
173. Cybersecurity and Infrastructure Security Agency. Cybersecurity Threats and Best Practices for Healthcare System, CISA.
174. Hu J, Jiang H, Chen S, Zhang Q, Xiao Z, Liu D, Liu J, Li B. Wishield: privacy against wi-fi human tracking. IEEE J Sel Areas Commun, 2024.
175. De Feo L, Leroux A, Longa P, Wesolowski B. New Algorithms for the Deuring Correspondence: Towards Practical and Secure SQISign Signatures, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 14008 LNCS, pp. 659–690, 2023, https://doi.org/10.1007/978-3-031-30589-4_23
176. Ghimire B, Rawat DB. Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things. IEEE Internet Things J. 2022;9(11):8229–49. https://doi.org/10.1109/JIOT.2022.3150363.
177. Lee ES, Zhou L, Ribeiro A, Kumar V. Graph neural networks for decentralized multi-agent perimeter defense. Front Control Eng. 2023;4:1–12. https://doi.org/10.3389/fcteg.2023.1104745.

178. Adigun GO, Ajani YA, Enakrire RT. The Intelligent Libraries: Innovation for a Sustainable Knowledge System in the Fifth (5th) Industrial Revolution, *Libri*, vol. 74, no. 3, pp. 211–223, 2024, https://doi.org/10.1515/libri-2023-0111
179. Bajaj S, Bopardikar SD, Von Moll A, Torng E, Casbeer DW. Perimeter Defense Using a Turret with Finite Range and Startup Time, *Proceedings of the American Control Conference*, vol. 2023-May, pp. 3350–3355, 2023, https://doi.org/10.23919/ACC55779.2023.10155838
180. ISACA. Third-Party risk management framework for healthcare. ISACA, 2023.
181. International Organization for Standardization. ISO/IEC 27701: Privacy Information Management, ISO/IEC 27701.

Publisher's note