Computer Networks and Communications
https://ojs.wiserpub.com/index.php/CNC

UNIVERSAL WISER
PUBLISHER

Review

Security and Privacy of Wearable Wireless Sensors in Healthcare: A Systematic Review

Ranjit Kaur[*], **Seyed Shahrestani, Chun Ruan**

School of Computer, Data and Mathematical Sciences, Western Sydney University, Penrith, Australia
E-mail: 18166138@student.westernsydney.edu.au

Received: 31 October 2023; **Revised:** 18 December 2023; **Accepted:** 4 January 2024

Abstract: Wearable Wireless Sensor Network (WWSN) devices are widely used in healthcare to monitor health data. However, when WWSN users transmit their data to healthcare professionals or third parties over wireless connections, they face privacy and security vulnerabilities. This paper aims to identify the unsolved privacy and security challenges in wearable sensor devices in healthcare, especially the aspects overlooked by previous research. The main research question is: What are the unsolved privacy and security challenges in wearable sensor devices in healthcare, and what are their implications for users and healthcare professionals? This systematic review employs specific keywords to search for relevant publications on bibliographic databases, including Google Scholar, Scopus, IEEE Xplore, and Web of Science. The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) charts helped in screening and summarising the selected papers. The results highlight the critical areas that can make WWSNs vulnerable to security attacks. The findings examine the security and privacy issues of wearable sensor devices in cloud computing, fog computing, the Internet of Things (IoT) and the like. Many studies examine IoT due to its privacy and security challenges, especially regarding handling extensive data, using public channels, deploying advanced technologies, managing sharing policies alongside the growing number of wireless devices, and protecting data from hackers. These challenges seriously threaten the confidentiality, integrity, and availability of health data transmitted by WWSN users to healthcare professionals or third parties in cloud-based environments and IoT and are exacerbated by limited resources. The significant findings thereby focus on unresolved areas in IoT. This paper aims to safeguard against cyber-attacks on healthcare and increase users' adoption rate of WWSN devices.

***Keywords*:** wearable sensor, privacy and security, healthcare, data management, Internet of Things (IoT)

1. Introduction

Wearable Wireless Sensor Network (WWSN) devices are attached to the human body to collect real-time health data and send them to healthcare providers [1]. The wireless Body Area Networks enable easy transfer of health data from one site to another, regardless of the distance between the parties [2]. The WWSN provides numerous advantages, such as remote access to data, real-time data sharing, portability, ease of use, and the ability to save time and money by avoiding the need to visit the hospital for routine check-ups [3]. However, security vulnerabilities associated with online or remote data sharing from wireless devices are widely recognised, with the potential for this sensitive data to be stolen by cybercriminals being an increasing concern [3, 4]. Privacy and security breaches in healthcare may majorly affect human life and potentially result in life-threatening attacks [5], especially as cybercriminals can add, erase, or modify the original

DOI: https://doi.org/10.37256/cnc.2120243852

information on a person's health record [6]. To address this risk, new smart approaches to identify security weaknesses in WWSN devices must be developed [7].

The security challenges involved in healthcare data storage are widely acknowledged. Over recent years, the healthcare sector has undertaken a wide range of activities to reach wider audiences since reaching them out physically became difficult during crises like COVID-19. The sector used multiple technologies and digital approaches dependent on software or online platforms to achieve this. These processes further increase cyber-attack risks since the systems are vulnerable. It is anticipated that securing the data generated in healthcare sectors by 2025 will become a great challenge on the Internet of Things (IoT), with any negligence in authentications in IoT potentially allowing security attacks [8]. Furthermore, privacy and security attacks continuously grow in healthcare regardless of various solutions provided [9, 10].

A further challenge is providing safe and secure transmission while multiple users handle patients' medical information in an emergency [11]. Attackers often successfully breach digital healthcare systems' security and privacy measures [12, 13]. This is because current healthcare technology systems cannot meet all the requirements of the latest systems due to the rapid pace of changing technologies, limited resources, energy and systems' limited capacity to handle large data [14]. For example, a survey undertaken among 106 WWSN users found that the majority were unaware of data breaches via unauthorised access to their sensitive data. To have enough knowledge to protect their data from such security vulnerabilities, users must be educated about using wearable sensors [15].

Furthermore, the literature shows that rules, regulations, and standards are not strong enough to protect health data. Manufacturers of smart devices do not follow all the safety and data security standards while producing wearable sensor devices [16]. Moreover, some wearable sensor devices are not appropriately designed, with data leaking from them [17]. Weaknesses in the inbuilt storage data make WWSN vulnerable to data breaches and corruption of the inbuilt storage data [18], as does the large volume of devices within the healthcare system. Third parties may also neglect to gain consent from the data owner before sharing the data, which leads to privacy and security issues. These issues are compounded by the extreme difficulties the latest technologies create for doctors in understanding and handling bulk patients' data and how best to keep it safe in future [19].

Furthermore, the outcome of the issues in the context of sharing data and monitoring health data with the help of intelligent wearables leads to the increased exposure of patients' information and patients' privacy concerns [20]. Apart from that, the benefit of using a wireless connection for healthcare professionals is that, since it presents accurate medical records of the patients, it helps with the analysis and management of continuous vital signs and transmits the information with the help of medical equipment. In the perception of [21], collected patient data leads to ongoing vital signs where wireless technology and appliances present a significant opportunity for managing real-time databases among the patients. Data integrity is the biggest challenge as attackers can mishandle data and information. Research has shown a substantial vulnerability in WWSN devices regarding cyber security in the healthcare sector [22].

Blockchain is a new technology in the healthcare sector, and many people are not aware of the respective benefits in the context of privacy and security for healthcare data. This is a complex technology, but there must be a short trial before the implementation. Combining the technologies can be challenging as they have different architectures and protocols, such as IoT and Blockchain, IoT and cloud, Fog computing and IoT, and Blockchain and lightweight. Combining the technologies with the WSNs can increase the risk of cyber-attacks and data breaches. This can also lead to scalability issues as adding new devices and sensors to the network can be difficult. It can also impact energy efficiency and battery life. Data reliability is also questionable due to the complex infrastructure and interdependence.

Utilising these combined technologies leads to significant vulnerability regarding cyber security in the healthcare sector [22]. In forgery attacks, a valid signature is created by someone else on health-related messages [23]. They take control of the whole message by adding a signature to it. Medical identity theft can be one of the most effective forms of attacks where one uses confidential information, such as the social security number, without the owner's permission, and makes false claims towards the process of Medicare and aggressive thefts of online medical cards. These forgery attacks can also cause problems with medical treatment [24].

1.1 *Research approach*

We use a systematic review methodology, a well-established technique that assists in identifying studies that discuss a common phenomenon [25]. Our review includes exclusion and inclusion criteria for selecting specific publications to ensure the information addresses the research motivations. We use this approach to explore the security and privacy challenges and their management in the healthcare sector, the most targeted sector for possible attacks on users' sensitive data compared to any other area.

In more detail, the study focuses on the following three areas:

- Research focus 1—Investigating different WWSN technologies used in transferring recorded data, identifying existing privacy and security challenges for users, and sharing health data using wireless connections in WWSN devices technologies.
- Research focus 2—Investigating the reasons behind the security challenges in wearable sensor network devices in healthcare. This paper focuses on analysing the causes of security vulnerabilities in wireless sharing.
- Research focus 3—Investigating solutions previously proposed to overcome these privacy and security flaws in WWSN devices in remote sharing and reviewing advanced technologies and the combination of technologies that may assist in securing health data.

1.2 *Research contributions*

WWSN devices may rely on IoT, fog computing, cloud computing, and the like. While these technologies play a crucial role in healthcare, limited research discusses or proposes potential solutions to strengthen their recognised vulnerabilities to make them more secure against cyber-attacks. This research addresses these gaps and critically mines the factors that make WWSN data vulnerable. It achieves this by conducting a systematic review of relevant scholarly articles published between 2017 and 2022 (inclusive) to identify security vulnerabilities in critical areas and to propose some solutions to enhance the security of WWSN for users, medical practitioners and healthcare settings.

Research Question 1 examines the privacy and security issues of WWSN devices. These occur due to vulnerabilities in methods or technologies. The answer to this question provides a detailed description of the reasons for such security challenges. It also assists us in analysing and finding security flaws in the healthcare system. Furthermore, Research Question 2 aims to explore all the offered solutions and compare the security issues. It provides more significant insights into healthcare, highlighting areas still not covered in the proposed solutions.

Most importantly, Research Question 3 shows the security risks after cyber-attacks on health data. This answer will also bring attention to those areas that are impacted due to malicious attacks. The paper is organised across four sections. Apart from this Introduction section, Section 2 details the systematic review methodology and the PRISMA approach used to identify the most relevant articles to be included in the review. Section 3 represents the obtained results. Finally, Section 5 concludes the findings and the recommendations for future direction.

2. Materials and methods

The systematic review associated with this paper aims to analyse previous studies and collect in-depth information about privacy and security issues in healthcare. It also aims to reduce bias and use explicit methods to conduct comprehensive reviews [26]. It is based on carefully selected criteria that guide the systematic search of the papers that cover the research questions.

The first step is to stipulate the research question using PICO (Population, Interference, Comparators and Outcomes) as this study focuses on a specific area; the next step is to use the keywords for search engines, such as Google Scholar and Scopus, and filter the papers using inclusion and exclusion criteria [27]. According to [28], the PRISMA diagram is followed in a systematic review as it includes multiple steps to find closely relevant papers. The steps are as follows:

A literature search on multiple databases, such as Scopus, Google Scholar, Web of Science and IEEE Xplore;

Use of specific keywords;

Use of Boolean operator strategies;

Use of similar keywords.

Table 1 represents the search criteria based on specific keywords and Boolean characteristics in four databases—Google Scholar, Scopus, IEEE Xplore, and Web of Science.

Table 1. Search strategies criteria for utilised databases

Search Engine	Keywords
(Google Scholar)	privacy and security "challenges OR concerns OR issues" in "transferring OR transmitting" the data in wearable sensor
(Scopus)	wearable AND sensor OR WWSN AND privacy OR security AND transmit OR transfer OR send AND health OR personal AND data.
(IEEE Xplore)	wearable sensor AND privacy OR security issue AND health data
(Web of Science)	wearable sensors AND transmit or transfer AND health data AND privacy OR security concerns

Google Scholar has found 80 percent more papers than other databases. In contrast, Web of Science and Scopus have provided the most peer-reviewed articles in the literature in English [29]. Moreover, IEEE Xplore is a significant data source that provides the most inclusive and specific papers by applying filter methods in the present study [30].

Table 2 represents data from research papers that are selected for systematic review. It clearly shows that the number of studies increased from 2017 to 2022. In addition, it is also clear that most of the studies are in the form of journal articles followed by conference papers and book chapters. It also shows that conference papers have decreased over the years whereas the number of book chapters has increased.

Table 2. Final utilised research papers

Year	Conference Papers	Journal Papers	Book	Total
2017	2	4	0	6
2018	2	7	0	9
2019	4	12	0	16
2020	0	14	2	16
2021	1	28	3	32
2022	6	33	1	40
Total	15	98	6	119

Selection of the articles—First, the title and abstract of all selected papers were read with the application of inclusion and exclusion criteria. Some criteria were applied to exclude some papers from the selection. They include the following.

Exclusion criteria

- Irrelevant articles
- Unpublished articles
- Outside of the date range
- Duplicate articles
- Foreign language

Inclusion criteria

- Data range between years 2007 and 2022
- Peer reviewed data

- Data referring to the information transmitted from patient to healthcare
- Data referring to people or patients who are using wearable sensor devices
- Privacy and security concerns regarding health data
- Published papers (journal articles, conferences)

Following the PRISMA criteria, some data, which will be used for systematic reviews, will be abstracted from the selected papers. For example:

- The name of the author
- The year of publication
- The types of research

Interpretation and summary of finding—This section will show the answers to the research question.

Figure 1 depicts the PRISMA diagram used to review the papers for the screening process. This graph illustrates the number of papers identified without selection criteria and the number of papers included in the final evaluation after using inclusion and exclusion criteria. Finally, 119 articles are used for review through the meta-analysis approach.

Data Extraction steps:

1. After collecting data from different databases, duplicate papers are removed.
2. The irrelevant papers have been removed after reading their titles.
3. After reading the abstracts and conclusions, another filtering process was done, in which other areas, such as education, agriculture, and the like, were removed and only the papers regarding healthcare-related were kept.
4. In the final step, critical screening has been conducted by keeping the papers about wearable sensors and sharing health data.

The data published between 2017 and 2022 is shown in Table 3. It provides details on the methodology employed in previous investigations. According to Table 3, previous research has proposed solutions that address security concerns and improve the performance of managing health data with wearable sensors in healthcare. However, systematic review methodology has been utilised the least over time. This systematic review methodology was primarily concerned with IoMT. In contrast, one study examined fog computing, another ageing places, and the third published health data's privacy and security issues. Literature review and survey methods are the two most employed in past research papers.

Table 3. Methodology used in resources published from 2017 to 2022

Numbers	Survey	Proposed Solution	Systematic Review	Comprehensive Review	Literature Review
2017	2	4	0	0	0
2018	1	3	0	2	3
2019	3	8	0	3	1
2020	1	8	0	1	6
2021	4	14	3	4	6
2022	6	12	3	2	16
Total	20	49	6	12	32

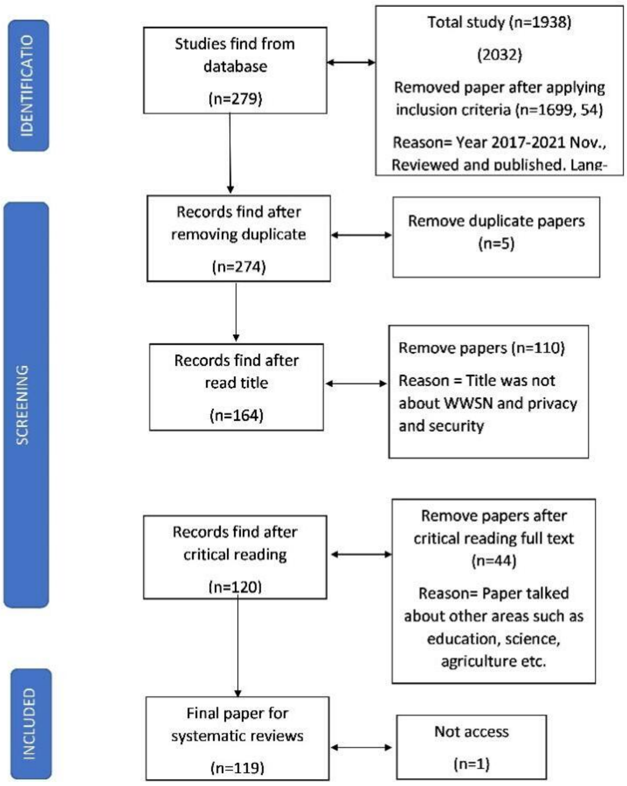
IDENTIFICATIO
SCREENING
INCLUDED
Studies find from database (n=279)
Total study (n=1938)
(2032)
Removed paper after applying inclusion criteria (n=1699, 54)
Reason= Year 2017-2021 Nov., Reviewed and published, Lang-
Records find after removing duplicate (n=274)
Remove duplicate papers (n=5)
Records find after read title (n=164)
Remove papers (n=110)
Reason = Title was not about WWSN and privacy and security
Records find after critical reading (n=120)
Remove papers after critical reading full text (n=44)
Reason= Paper talked about other areas such as education, science, agriculture etc.
Final paper for systematic reviews (n=119)
Not access (n=1)

Figure 1. Prisma diagram for the screening process

3. Results

The results review the current privacy and security challenges in healthcare. This section includes several vulnerabilities that create security issues for wearable sensor devices and discusses the causes of privacy and security problems.

Table 4 represents the vulnerabilities found in wearable sensor device methods and technologies. It includes the security and privacy challenges which happen in remote sharing. The following systematic review covers papers from the period 2017 to 2022 which are used for the analysis of the security issues in healthcare.

Table 4. Vulnerabilities of WWSN devices in healthcare

Methods or Technology	Weakness/Gaps/Disadvantages	Ref.
Internet of Medical Things (IoMT)	IoT faces cyber and malware attacks due to sensors and device vulnerabilities	[31, 32, 33, 34]
	Handling large amounts of data puts the data at risk	[35]
	IoT faces security challenges due to less capacity and scalability which result from limited resources	[36, 37,
	The IoMT system might affect patients' lives by causing privacy concerns about their personal information	38]
	Health data can be lost due to the lack of transparency and authentication, which may lead to data privacy breaches	[39]
	● Weak or default protocols are sometimes addressed ● Lack of awareness among stakeholders regarding the healthcare field and the knowledge of security vulnerability and cyber-attacks	[40, 41]
	90% of all IoT device traffic is unencrypted, which makes 57% of the devices more prone to threats that might reveal sensitive information	[42]
	Social network sites tend to share data inappropriately, which many users may use; providers have less confidence to store health data appropriately from threats; different policies are in different places regarding nationwide data sharing	[43, 44, 45, 46, 47]

Table 4. *Cont.*

Methods or Technology	Weakness/Gaps/Disadvantages	Ref.
	Conventional security issues in network technologies; possibilities of security attacks such as cyber-attacks, and privacy concerns; the attacker can capture the traffic and transfer it to its destinations by acting as a source	[48, 49, 50]
	Vulnerabilities in the user interface, network services, sensors, cloud services, and confidential threats	[51, 52, 53]
	At the time of data sharing, vulnerabilities are found in software and hardware	[6, 54, 55]
	Unchangeable passwords, unsecured web applications, lack of data storage and transmission security, encryption methods and network services	[56]
	● It is easy for hackers to access individuals' medical records transformed into digital ones ● The wireless disruption delays and creates interruptions due to poor signal, intermittent connectivity, unexpected disconnection, and slow network	[57]
	● Data integrity has been considered the most significant challenge as attackers can misuse data and information ● The utilisation of IoT and communication-relied protocols, including HTTP, MQTT, and many others, can lead to security threats	[58]
	● The implementation of data is quite challenging due to unawareness of methods ● Intensive techniques are not impactful in a continuously transforming environment ● Failure is possible due to maximising the allotted bandwidth of individuals in the context of sharing healthcare data	[59]
Fog Computing	Fog computing faces privacy issues because of insecure channels whereas handling a large volume of data also creates time-latency issues	[60]
	Issues in authentication protocols, privacy and security load balancing and offloading chores, and in implementing various hardware and communication technologies	[61]
Wireless Body Area Network	With some vulnerabilities found in International standard IEEE 802.15.6, WBAN is also not secure to fight against malicious attacks.	[62]
	The lack of resources makes the encryption scheme unreliable when data is transmitted to third parties	[19]
	The existing scheme is not working correctly against threats as the security key can be found from transmitted parameters and senders' public keys	[63]
	Handling large amounts of data at the time of updating to advanced technologies	[64]
	Wireless body area networks are experienced in active and passive attacks	[65]
	Wearable sensors can be easily carried at any time and location due to their size and wireless connection. However, they allow one to connect remotely with an unknown contact, which can lead to security flaws	[66]
	Data sharing does not meet advanced technology scalabilities	[14]
	When a wearable or implant sensor is remotely connected to various machines, malicious attacks can happen with unwanted connections	[67]
Blockchain technology	Security concerns in public blockchain technology as it is accessible to everyone	[68]
	It has processing speed and scalability issues	[69]
	Data can be lost when a cloud server transfers health data to the blockchain; the third party may cause security issues when they need data	[70]
Lightweight authentication scheme	Data is saved in plaintext form in memory	[71]
Home Patient Monitoring IoT systems (HPMIoT)	Data security and privacy; integration of various devices and protocols; data overload and accuracy	[72]
	Handling large amounts of data at the time of updating to advanced technologies	[64]
	Wireless body area networks are experienced in active and passive attacks	[65]
	Wearable sensors can be easily carried at any time and location due to their size and wireless connection. However, it allows one to connect remotely with an unknown contact, which can lead to security flaws	[66]
	Data sharing does not meet advanced technology scalabilities	[14]
	When a wearable or implant sensor is remotely connected to various machines, malicious attacks can happen with unwanted connections	[67]
Medical Health (mHealth)	Wherever healthcare is used, central-based systems face cyber-attack challenges	[73]
Attribute-based encryption (ABE)	Weak encryption and decryption methods are the biggest concerns in managing sensitive information	[13]
Big Data	Due to centralisation, data can be copied and stored without time and space constraints, and with weak encryption methods	[74]
Cloud computing with IoT	The data and information that unauthorised individuals might abuse negatively impact the entire healthcare system	[75]

Table 4. *Cont.*

Methods or Technology	Weakness/Gaps/Disadvantages	Ref.
Internet of Nano Things technology	Internet of Nano Things technology experiences intentional and unintentional attacks	[76]
Wireless Technology	If electronic health data is not used appropriately, it can suffer severe consequences regarding privacy and security. Mobile ad hoc network systems still have security issues. Fake authentication messages on network infrastructure can cause DOS or DDOs attacks	[77]
eHealth	Minimum access control measures have explicitly been severe, like system timeouts, data access control, and many others.	[78]
Healthcare Technology	• Healthcare technology becomes a victim of malicious attacks due to the lack of effective performance of the innovative healthcare system • An attacker may destroy the IoT infrastructure by performing a skillful attack on AI models	[79]
	Security problems are faced because of unauthorised activities with patients' electronic records and a lack of system security	[80]
	Lack of cost-effective and smart healthcare sensors with the unstandardised IoT system architecture	[81]
	One of the significant healthcare issues that is emphasised is that patients' confidentiality in data management is quite sensitive and directly impacts patients' security and health	[82]
	The COVID-19 pandemic is associated with challenges, such as data regarding privacy and mental health issues	[83]
	Data reconstruction errors, perturbation, and many more hinder patient information securities	[84]
Reconfigurable Intelligent Surface (RIS)	• RIS can produce potential security threats in IoT • After implementing certain tests, it is proved that RIS signals are worse than earlier in IoT network	[85]

Table 4 presents mostly papers on the Internet of Things (IoT) and the Internet of Medical Things (IoMT). Regarding sensors, critical issues are often due to wireless communication protocols and infrastructure. Table 4 summarises the key challenges that researchers have identified, such as cyber-attacks [31], protocol vulnerability [72], and premature deployment of technologies such as blockchains [70]. Research between 2017 and 2022 in IoT and IoMT has widely recognised issues regarding data and user privacy and security. On the other hand, few papers reviewed privacy and security issues in Wireless Body Network Technology (WBAN). A few papers also analysed the healthcare sectors to determine how patients share their data with healthcare professionals and how it faces security vulnerabilities. The following Figure 2 points out the main concern areas that create privacy and security issues of WWSN devices in healthcare. It includes vulnerabilities in methods or technology, network infrastructure, unawareness, data handling and wireless sharing.

3.1 *Underlying technology-related concerns*

Firstly, IoT is vulnerable to cyber and malware assaults due to sensors and device flaws [31]. It has specific common network security issues [48]. IoT is widely accepted in healthcare, which assists multiple wireless technologies to connect remotely. However, these wireless connections create privacy and security problems.

The results in Table 4 illustrate that various reasons are considered, including the probable causes of malicious attacks in IoT. The main issues are due to the unawareness of using and handling WWSN technologies, weak policies, rules and regulations of sharing health data and vulnerabilities in network infrastructure, to highlight a few.

3.1.1 *Handling large amounts of data*

Due to insufficient computing capacity and memory space in IoT, handling massive amounts of data can put the data in danger [35, 36]. According to [54], due to vulnerabilities in the user interface, network services, sensors, and cloud server, data breaches happen, which causes the leaking of confidential information, and which is a threat during data exchange [52]. Additionally, IoMT faces security challenges due to handling large amounts of data, weak policies, procedures and authentications [35, 38]. Lack of understanding and unawareness of using IoMT technologies create a severe concern [40].

Furthermore, IoT medical devices are becoming more common, but this can be a problem for users because it is a new and complicated technology which they cannot understand how to use [10]. According to certain studies, IoT vulnerabilities can occur in the user interface, network services, sensors, and cloud services, and unauthorised individuals can gain illegal access to them [51]. Additionally, data exchange in IoT is feasible when internal and external devices are connected via the internet, but software and hardware vulnerabilities might result in harmful attacks during interaction [54].

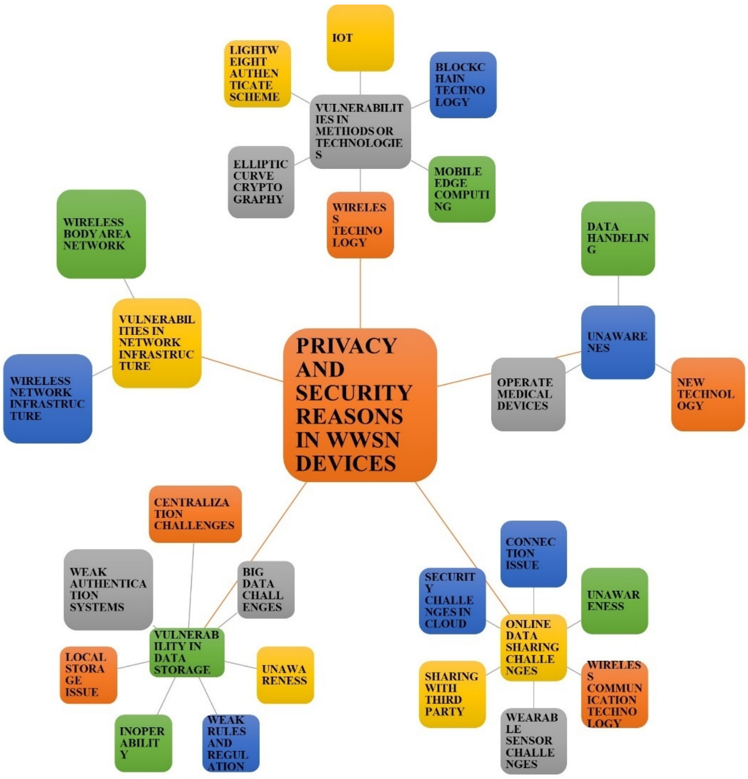
IOT
LIGHTWEIGHT AUTHENTICATE SCHEME
BLOCKCHAIN TECHNOLOGY
VULNERABILITIES IN METHODS OR TECHNOLOGIES
ELLIPTIC CURVE CRYPTOGRAPHY
MOBILE EDGE COMPUTING
WIRELESS TECHNOLOGY
WIRELESS BODY AREA NETWORK
DATA HANDELING
VULNERABILITIES IN NETWORK INFRASTRUCTURE
WIRELESS NETWORK INFRASTRUCTURE
PRIVACY AND SECURITY REASONS IN WWSN DEVICES
UNAWARENES
OPERATE MEDICAL DEVICES
NEW TECHNOLOGY
CENTRALIZATION CHALLENGES
CONNECTION ISSUE
WEAK AUTHENTICATION SYSTEMS
BIG DATA CHALLENGES
SECURITY CHALLENGES IN CLOUD
UNAWARENESS
VULNERABILITY IN DATA STORAGE
ONLINE DATA SHARING CHALLENGES
LOCAL STORAGE ISSUE
UNAWARENESS
SHARING WITH THIRD PARTY
WIRELESS COMMUNICATION TECHINOLOGY
INOPERABILITY
WEAK RULES AND REGULATION
WEARABLE SENSOR CHALLENGES

Figure 2. Privacy and security issues areas of concern

3.1.2 *Vulnerabilities in WWSN technologies*

On the other hand, blockchain technology is the latest technology that brings smart contracts and procedures to the market and provides solutions to various security concerns. However, it has been discovered that if public blockchain technology is used, privacy and security concerns may arise because anyone can access it [68]. When data management is not regulated, tracking and managing it can lead to breaches. Moreover, blockchain technology has some challenges, such as processing speed and scalability, when compared to traditional database systems [86] where users may have concerns about security when managing distributed ledger systems and data synchronisation technologies [34].

Apart from that, security concerns in fog computing include authentic protocol implementation, privacy and security load balancing, and the implementation of various hardware and communication methods [61]. Because wireless communication technology has fewer resources to enable robust encryption, it can potentially cause data leakage [87]. Elliptic curve cryptography has previously been discovered. According to it, some security weaknesses can be noticed in the existing ECC, including DDoS assaults, a key compromise issue, a stolen verifier attack, a lack of remote forwarding, a lack of control over security keys, and a lack of time synchronisation.

A lightweight authentication scheme was also introduced to enable data transmission from wearable devices to healthcare servers. This research has discovered security issues, such as stolen wearable device attacks, in which attackers can use the stolen device's memory and user impersonation attacks. The rationale for the preceding attacks is that data is stored in RAM in an unencrypted form, which makes it easily readable and hackable by attackers [71].

3.1.3 *Authentication challenges*

As the number of medical IoT devices grows, there is a massive lack of new ideas in less secure environments which run them [10]. Patients, healthcare providers, and others working on it do not know about the security policies, standards, governance, and different rules and regulations of new technologies [10]. Sharing a device with family and friends and not using a password, encryption, or a secure cloud for most daily activities can lead to security breaches that users do not know about [73].

Privacy and security come under concern when there is time to adopt ePHR with advanced technology because users are not entirely sure how to use the system [3]. In the light of wireless communication technologies, users have little confidence in FL [88]. Concerns about data security arise when people are unaware of how to properly manage sensitive data when it is shared via wireless communication [3]. Moreover, the inability to identify user identification numbers of harms healthcare consumers because it contains personal information associated with their names [3]. Security and privacy vulnerabilities are the primary concerns in context-awareness systems as all personal information is transferred to third parties, which may result in the data being leaked to an unauthorised individual [89].

3.2 *Shared environments and connectivity challenges*

As a result of the lack of adequate connectivity, health data is still shared in hospitals in paper format; data is not available on time and is left open to the public [10]. Social networking services, which may be used by many people [43], are being used to share data inappropriately. Present-day healthcare does not meet or cannot scale up to the demands of advanced technology, and as a result, it lacks a structured data transmission system that is secure, dependable, and consistent [14]. Regarding data-sharing policies, different policies are in effect in healthcare [43]. When consumers are not aware of how to manage sensitive data when it is shared over wireless communication, this is a grave security problem that needs to be addressed [3].

3.2.1 *Vulnerabilities in wireless technology*

The primary risk with wireless technology is that data is transmitted across the air, with a high probability of sensitive material being copied by unauthorised individuals. Low-power wireless technology can also be a source of privacy and security concerns [90]. Anyone can use wireless communication technology, and intruders can launch attacks on network infrastructure such as DDOS and authentication attacks [91]. Also, remote access raises security risks for sensitive information in healthcare, including illegal entry, credential misuse, data loss, and record manipulation [8]. A WWSN device synchronises with mobile applications to transfer data to a third party, which may cause data hacking [92]. If Telecare Medical System's confidential data is exchanged via the internet, there is a chance of an attack by external systems [2]. When wearable sensors or implant sensors are remotely connected to various machines, then malicious attacks can happen with unwanted connections [67].

Furthermore, malicious assaults can seize control of the communication system during data transfer, and there is a considerable possibility of changing, deleting, and adding information and inaccurate health data records via public communication channels. As a result, the WWSN device is susceptible to the following attacks: denial of service, replay attacks, a man-in-the-middle attacks, offline password guessing attacks, smart-card-loss attacks, personal attacks, user anonymity attacks, and authentication attacks [47].

3.2.2 *Weak authentication systems in wireless technology*

Wireless communication over the public internet creates serious security concerns. When doctors handle extensive data from multiple patients, information addressing their privacy [93] can be leaked. The encryption scheme is unreliable for internet data transmission to third parties [19]. Internet data transmission is a big security challenge [94]. While using a wearable sensor device, one can find context privacy when the device shares data that the user does not want to be shared, and bystander privacy when some wearable devices capture the data and information from their surroundings. It is said that when a wearable sensor or an implanted sensor is remotely connected to several machines, malicious assaults can occur as a result of the undesired connections made by the sensors [55]. Transferring data from sensors to the cloud via IoT can raise security concerns [53].

Code injection attacks are possible on the Internet of Things due to cloud vulnerabilities [52] when end-users share and access data. When data is transferred from sensors to healthcare servers via hybrid cloud systems, including public or private cloud systems, security concerns for users and physicians can arise [69]. Data breaches are highly dangerous because data is transmitted over public cloud servers [11]. Furthermore, when cloud servers send health data to the blockchain, data can be lost. Although the cloud server stores data using robust encryption methods and different cryptography systems, a third party may introduce a security risk during transmission [70]. Cloud-based data is vulnerable to various threats, including malicious attacks, data manipulation, and privacy and security breaches. Attackers may utilise patient data [95].

3.3 *Operating system challenges in healthcare*

As the number of devices is increasing in medical IoT, the domain still lacks innovation and has a less secure environment for safe execution [10]. CPS has security concerns; its primary challenge is its relation to advanced technologies. It causes many malicious attacks. New technology and innovation need new policies before implementation; otherwise, they can cause physical security attacks in healthcare [96].

3.3.1 *Centre-based health system concerns*

Natural outbreak threats or attacks and biological attacks can happen in health data because these attacks are extremely hard to be analysed and detected simultaneously when they occur [12]. Healthcare service providers lack interoperability [97]. Insecure and weak authentication may cause security attacks, such as data injection on health data [98]. The former health system is a center-based system with security vulnerabilities where attackers can easily control wearable sensor devices and delete, change, or add data [73].

Due to centralisation, privacy and security concerns about health data remain. In contrast, previous mHealth systems were center based with security vulnerabilities, allowing attackers to easily take control of wearable sensor devices and remove, edit, or add data [74]. If electronic health data is not used effectively, it can have significant privacy and security implications [77]. Additionally, data ownership is a substantial issue because users are unaware of how to use or share data, and data transmission, such as when users send data via email, can generate privacy concerns [99].

3.3.2 *Weak policy and regulation in healthcare*

Regarding data ownership, there are no standards or protocols in place; for example, there are no rules or regulations governing who has responsibility for the information [44]. While any systems or technologies are being deployed, data can be compromised. For example, radiofrequency collects data that cannot be captured optically by a regular camera; partially processed data requires extra technology, which can also be a source of security issues [100]. So, malicious attacks on data integrity are also common [87].

Moreover, some wearable sensors store data in a local storage, which does not employ encryption or data protection measures, and this can result in data loss in certain circumstances [92]. Data from various sensors, such as smart devices, smart watches and wearable sensor devices, can be complicated to handle, analyse, process and store [97].

3.3.3 *Cloud server security risks*

In a cryptography system, if the key is revealed, it is impossible to keep the data safe [101]. When a cloud server transfers health data to the blockchain, data can be lost. Although a cloud server has stored data using robust encryption methods and different cryptography systems, third-party interference may cause security issues during the transmission [70]. As a result, there are some possible attacks when users want to obtain raw biological data from sensors as there is an opportunity for unauthorised people to interfere [102]. If the authentication is not accessed correctly, data encryption and decryption techniques will be delayed, and there is a strong chance of DOS attacks [103]. Cloud-based data faces many challenges, such as malicious attacks, manipulation of sensitive data and privacy and security breaches, and intruders may use patients' data [95].

The database is not fully secured because it has its limitations. Research confirms that digital signatures, used to exchange information, can have vulnerability-causing forgery attacks [17]. Storing data in the public cloud increases security and privacy concerns. If there is a single failure, a third party needs to handle or solve such issues, which can lead to the leakage of health data [104].

If personal health records (PHR) are stored in the cloud as plain text, they are vulnerable to malicious attacks. Attribute-based encryption (ABE) method is used for fine-grained access control and search encryption key for encrypted data, but it has a security loophole that shows that data is not safe with these methods [13]. Handling enormous amounts of data may put the data at risk [35]. Providers have less confidence in storing health data appropriately from threats [43].

3.4 *Vulnerabilities in network technologies*

A mobile ad hoc network system still has security issues. Fake authentication messages on network infrastructure can cause DDoS attacks [77]. WAN gateway includes wireless routers, access points and wireless connection, allowing to connect with other networks with data traffic issues, which can cause security breaches in data transmission handling [105].

3.4.1 *Challenges in handling large network infrastructures*

Previous WBAN architecture dealt with large amounts of data, but this can create complexity and cause security and privacy challenges for users; updating or implementing new technologies can also cause data confidentiality and integrity issues [64].

Wireless communication methods and large-scale network use are the most significant security vulnerabilities [9]. A security concern relates to Wireless sensor network, Machine to Machine communication and cyber-physical system in IoT [50]. An insecure wireless connection can cause brute-force attacks [92]. Data can be exchanged in WBAN because it lacks restrictions and has a mobility feature, as we can carry it anywhere/anytime. All these reasons can make it easy for intruders to attack data [66].

3.4.2 *Malicious attacks*

WBAN is also not secure when fighting against malicious attacks such as DOS, man-in-the-middle, and impersonation attacks. So, authentication and confidentiality are crucial in WBAN [62]. Lack of resources and consumption can cause malicious attacks in WBAN [19]. WBAN, as a wearable device, collects remote data and transfers it to caregivers and, with fewer authentication systems found, this leads to security and privacy attacks. The existing scheme is not working against threats as security keys can be found from transmitted parameters and senders' public keys [63].

Therefore, wireless sharing across a public channel generates malicious assaults, authentication attacks, and other attacks based on the activities of individual users [6]. In addition, it was discovered that unchangeable passwords, insecure web applications, and network services contribute to healthcare security breaches. Limitations in computing speed, memory space, and comprehension of input and output functions have posed security threats to the IoT [38].

Overall, the results illustrate that privacy and security challenges are mainly discussed in IoT and IoMT areas. The significant reasons for this are unawareness of using the technologies and methods, handling large amounts of data, limitations in wireless connections and weak policies, standards and authentications. Moreover, the healthcare network structure cannot ignore the security attacks by unauthorised people who use fake source IDs.

3.5 *Impacts on users and systems*

3.5.1 *Health data stealing or monitored information leakage*

This paper states that human data has been changed due to data stealing from the server by unauthorized people. From various sources, it has been established that over 500 data records have been stolen, and the average amount of stolen data increases weekly to a new record. Data privacy maintenance can be a security concern within the Healthcare society. Moreover, it is defined that data maltreatment can lead to due to lack of efficiency in healthcare organizations, and it can create massive losses for healthcare in terms of finances as well as Service Delivery [106]. It can be stated that data and privacy challenges are primary when information about patients' leaks is monitored. Hence, these problems exist with RFID technologies [100]. Operations from a central security point of view can be regarded as one of the most essential notions within the business. Creating efficient control solutions is vital for increasing the potential for blockchains and decentralising the different technologies. It can be stated that the decentralization of data is an important case to prevent health data misuse.

3.5.2 *Control of security keys and time synchronization issues*

The critical control methods tend to encapsulate the different facts, not the absolute control lost due to unauthorized users keeping track of the company keys. It allows the information to be used by authorised people only and processed as a tethered or locked key cabinet. A signed key control agreement can be regarded as one of the preventive measures for controlling security keys. However, secure synchronisation and data sharing cannot be possible without cryptographic seniors. Scrambling and unscrambling of data can be regarded as highly necessary for maintaining control over their keys. Potential security keys and shuffling of the remaining part can be considered as one of the primary attributes and can create extra security protection, reducing time synchronisation issues [11].

3.5.3 *Secret forwarding*

It can be stated that the provision of perfect secure forwarding can be regarded as highly important because it can alter the encryption system and ensure that a minimal amount of sensitive data is breached, even if a key is hacked. Perfect forward secrecy stops man-in-the-middle attacks and multiple attempts to back up and decode sessions during the secret sending process.

It can be stated that the secret key can be regarded as an essential aspect that can determine the monitoring systems. The generated secret key forwarding has been used to follow the encryption formula. When subtracted from the decryption value, it can help create the security that has always been necessary within the healthcare system [95].

3.5.4 *Misuse of patients' data and personal information*

It has been observed that attackers use patients' data and personal information to create phishing or impersonation threats to the ones from whom data has been collected. It can be stated that the information collection without consent can lead to other data misuse. Unlike an ethical breach, it can be noted that in the case of no one hacks the data, but the attaches occur due to company's partners or to policies regarding data sharing. There have been several intrusions that need to be reduced on a manual basis, and a high degree of similarity cannot be detected. The misuse detection model can act as a verification model which verifies any anomaly that can be detected. Also, the classification of several intrusions can be regarded as one of the most viable processes, and it is based on the intrusion signature. It can reduce the rate of false negatives. False detection of different anomalies can also be highly significant [8].

3.5.5 *Privacy reveal and false information transmission*

It can be stated that ensuring patients' privacy is one of the clinical necessities for healthcare professionals. Also, patients always are entitled to the right to maintain privacy, and a notice of privacy is a necessity and has been acknowledged by HIPAA [107]. It can be stated that privacy can be revealed by external attacks if any phishing or data breaches using Trojans or other viruses occur, or if the sharing policies of healthcare practices can be disclosed.

As big data and other various technologies store patients' information on medical health and medical activities, this can be regarded as one of the most significant factors and generate different financial information. Also, the 5 V features in big data can contribute to maintaining privacy in data security within healthcare [74].

3.5.6 *Resource-efficient authenticated data sharing mechanism for smart wearable systems*

This paper has found that Blockchain technology is widely recommended for use in healthcare to protect healthcare data. Due to smart contracts, blockchain provides safe and secure data sharing in healthcare [108]. The study also advises the use of cyber-physical systems in blockchain technology, but they are not used in real scenarios. Moreover, blockchain technology is very expensive and time-consuming to protect health data during implementation in IoT. The paper shows concerns if blockchain needs its smart contract changed, which may cause vulnerabilities [109]. IoT devices cannot handle privacy and security challenges due to a lack of in-built security features [110]. A recent study has explored the fact that public blockchain technology cannot handle data efficiently in healthcare as anyone can access it [111]. Apart from that, healthcare data used for training and testing face security concerns in healthcare [112].

3.5.7 *Resource-efficient authentication scheme for telecare medical information system*

The current study has concluded that 6G is a wireless communication network which provides secure, fast and energy-saving connections [113]. Researchers have proposed a solution with the combination of Federal learning with cloud computing and fog computing named FedSDM [114]. It plays a crucial role in enhancing security among healthcare providers in IoT, but future research is needed on energy, resources, and outcomes for its use in the healthcare sector.

3.5.8 *The use of formal verification and validation techniques in IoT*

The findings indicates that formal verification and validation techniques can improve the services of IoT in handling health data. However, it is a big challenge for researchers to provide strong formal verification and validation systems because IoT has a very complex framework which includes different types of communication channels to connect different points. A recent study explores how a formal verification and validation system is implemented in IoT. Firstly, it ensures that the appropriate protocols should be used in IoT. Secondly, it is necessary to ensure verification of the security properties which enhance the secure connection among users while sharing data in IoT. Moreover, it is important to propose strong protocols to address the falsified identity which can be found during verification techniques. Lastly, certain tests on the protocols are implemented to enhance the test.

4. Discussions

This section provides an overall summary of the privacy and security results. It describes significant findings and many concerns that need future reviews. This paper is focused on finding security vulnerabilities in health data that are shared in an online mode with healthcare professionals. Health data faces several security and privacy challenges, which can lead to numerous life-threatening concerns. The following paragraphs highlight the main areas that need future attention to provide safe health-sharing environments for WWSN users.

This paper has found that the methods and technologies used in healthcare to handle WWSN devices' data are facing security issues. This paper targets the health sector to analyse the answer to the first research question. According to Figure 3, from what has been examined in the systematic review methodology, this study can conclude that some methods and technologies are unsafe for sharing or managing health data remotely. The data can face malicious attacks for several reasons, as discussed in Sections 3.4 and 3.5. The technologies that can be affected include IoT or IoMT, blockchain, fog computing, cloud computing, lightweight systems, WBAN, eHealth, and the like.

Secondly, previous studies have shown that healthcare faces privacy and security issues in WWSN devices, and they target IoT or IoMT because they are widely adopted in healthcare sectors. Figure 3 depicts the privacy and security concerns raised by WWSN technologies used in wearable sensor network devices to share data from users or patients to healthcare experts remotely.

Moreover, Table 4 shows that this research explored IoT for the period from 2017 to 2022. Although most papers target another sector, IoT has been widely analysed. In addition, blockchain technology regarding privacy and security challenges in healthcare for handling WWSN devices was first examined in 2021. It is predicted that future studies will widely cover blockchain technology as many papers recommend it as a solution. For example, Table 4 indicates that blockchain also has some security vulnerabilities as it faces cyber-attacks challenges in adopting public chains that anyone can access.

Moreover, blockchain technology is not mature enough to handle health data in the healthcare sector. Public blockchain cannot solve the issues if users can use public connections or channels to share sensitive data with health professionals or third parties. It also cannot be secure when a cloud server transmits the data with a blockchain.

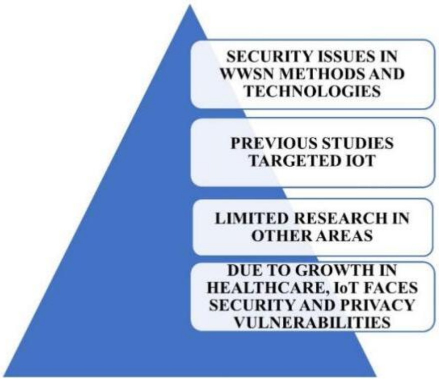
SECURITY ISSUES IN WWSN METHODS AND TECHNOLOGIES
PREVIOUS STUDIES TARGETED IOT
LIMITED RESEARCH IN OTHER AREAS
DUE TO GROWTH IN HEALTHCARE, IoT FACES SECURITY AND PRIVACY VULNERABILITIES

Figure 3. Major findings (IoT)

The above findings include privacy and security vulnerabilities and the solutions offered in previous studies, as well as risks to the healthcare sector, and vulnerabilities in communication technologies that are used in sharing health data. This study is focused on finding security vulnerabilities in health data that is shared in an online mode with healthcare professionals. Health data faces several security and privacy challenges, which can lead to numerous life-threatening concerns.

Table 5 compares security challenges and offered solutions, clarifying the unresolved and resolved areas. It also shows what sorts of solutions are advised by the researchers. However, a lack of secure execution, unawareness of using the services, social or public sites, weak policies, and third-party sharing are not covered in terms of privacy and security issues.

When advanced technologies are implemented in healthcare, they do not meet the scalability requirements due to the lack of resources, which also does not advise robust solutions. As IoT can connect several devices each year, and the number of interconnected devices is growing. These interconnected devices collect, analyse, store and exchange health data with healthcare providers using wireless network connection channels, either public or private. Previous studies have proposed ideas to cover the gap in handling many IoT-connected devices. One of the studies finds that satellites and unmanned aerial vehicles (UAV) are used together in IoT to manage many growing IoT devices [115]. On the other hand, satellites and UAVs send information to the cloud, but the cloud is a central administrator to collect and process information together. Moreover, the study does not state if this approach can be implemented in the healthcare sector and if it is safe to manage large amounts of data securely. Therefore, this brings privacy and security challenges in healthcare as unauthorised access exposes the WWSN devices to risks, such as malicious attacks on healthcare.

Table 5. Comparison of past offered solutions with present security issues

Reason for Security Concern	Status		Solutions
	Yes	No	
Vulnerable medical device	✓		Recommendations
Lack of secure execution		✓	
Lack of awareness of security		✓	
Insecure encryption and decryption	✓		• Cryptography system • Integrated Circuit Metric Algorithm • Zig Bee technology • Efficient Lightweight Trust Assessment Scheme
Weak authentication systems	✓		• Lightweight Security Biometric technique • Telecare Medical Information System (TMIS) • Lightweight autonomous authenticated & key agreement scheme
Social network sites are used to share data inappropriately, which can make it accessible to many users		✓	
Lack of standards, regulations or policy, and legal issues		✓	
Providers have less confidence in storing health data appropriately and protecting it from threats	✓		• Blockchain • Recommendation—Symmetric Key protocol
A security concern comes when sensitive data is shared with a third party		✓	
Lack of use of patients' unique identification		✓	
Updating or implementing new technologies		✓	
Privacy and security concerns due to centralised technology in healthcare	✓		Blockchain
Mobile ad hoc network issue	✓		
Data sharing with the third party	✓		Context Awareness Scheme
Data sharing via Wireless communication	✓		• Interoperability as a property (IAAP) method • WBAN technology & Zig Bee technology • Combination of Blockchain, Bluetooth, Machine Learning • Bluetooth communication & Public Key Infrastructure
Wireless Network technology or services	✓		MESH network & Blockchain
Handling large numbers of data	✓		Security keys
User has no ownership of their data	✓		
Software or hardware vulnerabilities		✓	
Time latency	✓		Combination of IoT and 6G
Insecure channels on the Internet		✓	
Data integrity		✓	
Cloud server (public)	✓		• Edge Computing & Fog Computing • Lightweight signature scheme with blockchain • Elliptical Curve Cryptography (IECC • Recommendation—scramble and descramble data • Recommendation—Hidden policy of Attribute-based encryption
Lack of resources		✓	
Weak protocols		✓	
Third-party interference		✓	
Security attacks	✓		• Combination of AI and machine learning • Combination of Transfer learning model and Blockchain • Mobile Edge Computing & Blockchain • Biometric authentication scheme algorithm
Handling a large number of devices in IoT	✓		A combination of satellites and unmanned aerial vehicles can communicate with multiple IoT-connected devices where rate-splitting considerable access assists in managing connection

Table 6 provides further detailed information, including the unsolved areas, the domains with security issues, and the details of why they are not resolved yet. It shows that all unresolved areas belong to the IoT domain, as discussed in Section 3.

Table 6. Unresolved areas in healthcare

Research Gap	Domain	Comments
Handling enormous amounts of data	IoT, Fog Computing, WBAN, MEC	Previous studies provide solutions to handle data safely. However, they do not explain how to conduct extensive data in remote sharing [35, 58, 60, 64, 88]
Using social sites	IoT	Solutions are about securing data transmission with third parties, but there are no solutions for protecting a social site while sharing data [43]
Using public channels	IoT, Blockchain, HWSN Public cloud	Previous studies do not provide a solution for public channels. Using a private blockchain instead of a public one is advised, as public one creates issues when moving data from the cloud to the blockchain. In public clouds, elliptic curve coding is recommended for protecting health data. However, this still needs future review in the case of handling complex data [47, 68, 69, 93]
Unawareness of handling data	HEIR, IoT	Lack of knowledge about how to use technologies creates security issues, but no solutions are offered to make users aware of these vulnerabilities [10, 38, 40]
Integration of various devices	IoT, HPMIoT	There are serious concerns as the number of connected devices for sharing and collecting data is increasing in healthcare sectors, and privacy and security issues are rising simultaneously. These are challenging areas for users, and there are no definite solutions so far [46, 72]
Overloaded data	HPMIoT	Blockchain and edge computing are offered as solutions for data handling, sharing and storing. These methods do not discuss protecting overloaded data from security vulnerabilities [72]
Secure sharing on the network	IoT	Combining satellites and cell towers improves efficient and secure transmission on wireless networks. However, the study implements the proposed solution on computer simulation models, but it still needs to be tested in real environments for accurate results [116]. Moreover, another proposed solution tries to enhance secure transmission by adding more multi-antenna-based stations, but this solution cannot be implemented in healthcare until it is tested in a real environment [117]

Although some other concerning areas cannot be ignored when protecting health data from attackers, introducing a new or advanced technology poses a security threat, according to this study. This occurs because new methods, technologies, or policies need updating before deployment, which does not reduce the security risks [96, 100]. However, this research has found no previously discussed solutions for addressing these limitations. In addition, a few studies have expressed concerns over the lack of policies and standards governing the remote sharing of health data with third parties. However, we have been unable to locate any proposed solutions to strengthen the rules and regulations that govern safe and secure remote sharing in healthcare [4, 43, 44, 46, 62].

Moreover, the health sector manages a substantial amount of data compared to other firms. However, privacy and security concerns can arise when enormous amounts of data are incorrectly handled due to limited resources and energy [14, 35]. Data sharing with a second and third party and storage on a cloud server and a healthcare server demonstrate that users no longer own their data [70, 92, 118].

This paper also covers various privacy and security risks in healthcare when malicious or cyber-attacks occur. These attacks are performed by intruders who target health data to misuse it, which can lead to severe consequences for users and healthcare professionals. A recent study shows that an intruder targets healthcare areas for cyber or malware attacks on healthcare, and this has been increasing over five previous years. Moreover, it also states that the healthcare sector is less sophisticated to face and prevent these attacks [119].

Furthermore, as mentioned in the results, IoT is widely adopted in healthcare as it connects many wireless connection devices. Therefore, IoT needs to handle a large amount of shared data, and it meets security risks when it cannot address security and privacy vulnerability issues in IoT. Figure 4 depicts the key findings, including that IoT faces the most malicious attacks since weak authentication systems, encryption and decryption methods, and insecure wireless connections cause such attacks. Moreover, it addresses the causes of vulnerabilities in a wireless connection, such as hijacking a trusted person's system to enter the whole network and creating a traffic jam in the network infrastructure to interrupt the network nodes and communication.

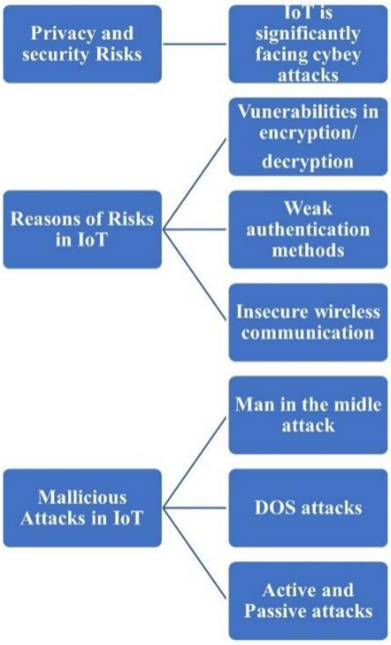
Privacy and security Risks
IoT is significantly facing cybey attacks
Reasons of Risks in IoT
Vunerabilities in encryption/ decryption
Weak authentication methods
Insecure wireless communication
Mallicious Attacks in IoT
Man in the midle attack
DOS attacks
Active and Passive attacks

Figure 4. Key findings in security attacks

Moreover, this paper also reveals that, according to previous studies, man-in-the-middle attacks, DOS, and active and passive attacks happen in IoT, in addition to security risks, attackers first try to steal the secret key and then use personal information to start communication with other nodes. This research finds that attackers target trusted parties (wearable sensor users and healthcare professionals) who communicate.

These risks seriously impact network infrastructure, communication technology, and medical devices. The primary key area shows that network infrastructure risks are the most concerning because they lead from one organisation to another. These systems are interconnected internally; attackers can find a way to enter another using security keys, stolen personal information, and the like if they target one network.

Overall, this research has found that unresolved security areas in WWSNs include third-party sharing, weak policies, handling extensive data, the increasing use of interconnected wireless devices, and a lack of understanding in managing health data with WWSN in IoT, fog computing, cloud computing, and WBAN technologies. While blockchain technology is promising, it still needs to evolve its capacity to be more useful in the healthcare sector regarding third-party sharing and warding off cyber-attacks. Additionally, wireless connectivity solutions must be more vital to provide end-to-end security due to limited resources as malicious attacks are increasing in the healthcare sector, which must be addressed.

The following Table 7 compares previous surveys and systematic review to analyse the gaps in the area that need attentions.

Table 7. Comparison of previous survey and systematic review

Systematic Review	Focus	Security Issues Discussed
[41]	The concerned paper delivers a critical analysis of the IoMT in the era of the Covid-19 phenomenon	Insufficient security knowledge among medical consumers
[84]	The concerned paper focuses on the importance of privacy and trust in the context of providing patients' health data and its protection with the implementation of proper legislation	Errors in data reconstruction, perturbation, and many more that hinder the security of patients' information
[120]	The paper has focus on understanding telemedicine technology in healthcare	The latest wearable technology allows users to access the data anywhere and anytime, which creates security vulnerabilities challenges
[121]	The paper focuses on examining physical activities and monitoring the data in healthcare	Not mentioned
[48]	The paper discusses the security issues in different architecture layers in IoT	Security issues in IoT domain that still need to be analysed carefully
[99]	The authors review Blockchain technology for healthcare services because it is found to be safe and secure technology to keep data free from security attacks	Examples of attacks: WannaCry attack in May 2017 which was a worldwide attack on health data; One more attack on Electronic Health Record in Los Angeles Moreover, data ownership is a big issue because users are not aware of how to use or share their data Data sending via email as a cause of privacy concerns Secondary healthcare is not able to maintain de-facto standard
[60]	Fog computing applications and challenges in healthcare are discussed	Insecure channel on the Internet Large data volume Time latency to provide response
[122]	Comprehensive review of smart home devices to provide safety, secure and reliable data transmission systems, and robots added to the existing technology to aid in physical activities	Eavesdropping attacks can cause data leakage
[61]	The motive of this paper is to conduct systematic review on Fog computing including application, challenges, architecture and quality of services	Fog computing contains some security issues: Authentication protocol Privacy and security load balancing and offloading chores Implementing various hardware and communication technologies
Survey		
[58]	This paper depicts various current security issues with their counter mission in the healthcare system	Data integrity has been considered the most significant challenge as data and information can be misused by attackers Utilization of IoT and communication-relied protocols including HTTP, MQTT, and many others is prone to security threats
[37]	This paper shows that blockchain has the potential to mitigate privacy and security concerns of fog computing by evaluating the issues, as well as challenges from the viewpoint of FC and IoMT	Capacity and scalability issues faced by IoMT IoMT system might affect the lives of a patient by causing privacy concerns about their personal information
[78]	The concerned paper discusses the importance of eHealth in the reduction of the negative impact of the pandemic on the healthcare system	Minimum access control measures that have been specifically severe, like system time outs, data access control, and many others Insufficient audit managing system
[32]	The paper highlights the significance of the Internet of Medical Things, as well as of digital healthcare systems, which help individuals in acquiring quality healthcare services at their individual homes	Lack of could security to safeguard health-related data and information
[49]	The concerned paper analyses the present advances in the use of IoMT with IoT healthcare systems	The attacker has the capability to capture the traffic and transfer it to its destinations by acting as a source
[79]	This paper demonstrates various smart healthcare technologies, like wearable devices, body area networks, and digital healthcare, along with their privacy components, as well as solutions for the smart medical system	Lack of effective performance of the smart healthcare system An attacker may destruct the IoT infrastructure by performing a skillful attack on AI models
[81]	This paper demonstrates a precise analysis of the significance of smart sensors, AI, IoT, and Blockchain in HMS to acquire a better understanding of the healthcare system.	Lack of cost-effective and smart healthcare sensors with the unstandardized IoT system architecture
[39]	This paper highlights the importance of artificial intelligence in the current advances in IoMT	Lack of transparency and authentication Data privacy breaches
[123]	This article discusses various aspects of IoT in healthcare, such as security systems, electronic health and mobile health, system architecture, cloud computing, fog computing, communication technologies, and others	Not mentioned
[46]	The objective of this paper is to review Blockchain technology in IoT for privacy preservation of health data	As IoT devices are interconnected, this can cause security threats such as: Denial of Service attack, fabrication of identity, physical attacks, and so on. Communication technology can also cause attacks Lack of standards in security

Table 7. *Cont.*

Systematic Review	Focus	Security Issues Discussed
[34]	This paper finds new security challenges in IoT which may be helpful for researchers, manufacturers, individuals and organizations	(There are other security issues as well, but this paper discusses only security issues in healthcare) Distributed denial service attack during COVID 19 and Mirai botnet attack in healthcare Security issues in blockchain standard such as managing distributed ledger systems and data synchronization systems
[50]	This paper encourages researchers to find out about blockchain technology for IoT, Fog computing, and Cloud computing because it is adopted by all sectors to save their data	Security concerns are related to Wireless sensor network, Machine to Machine communication and cyber physical system in IoT
[38]	The paper reviews IoT applications, technologies, protocols and security systems in healthcare	IOT security challenges: Restriction on computational speedMemory space limitation Lack of understanding of input and output functions

In the recommendations for wireless sharing, IoT requires end-to-end wireless connections, methods and techniques to maintain and stabilise the wireless connectivity and handle health data. Resources to operate these technologies on different platforms are also required. Robust authentication systems to access the WWSN devices and an encryption and decryption system are needed to share the health data from users to healthcare providers and vice versa. This research also recommends that healthcare workers need wearable sensor users' disclaimers before sharing data with a third person. It must be done in two ways to allow the users to understand the pros and cons of third-party sharing: face-to-face communication and a signature on the form because older people may not be aware of receiving the document or cannot read it. So, face-to-face communication or verbal communication makes understanding easier. Both parties should agree before proceeding; this policy can be saved both parties after this agreement. Regarding limitations, this research needs detailed information about how blockchain technology works in healthcare.

5. Conclusions

This paper examined wireless connection technology wearable sensor network devices to find security vulnerabilities in remote sharing in healthcare. Based on the systematic review methodology, this research has critically analysed previous research on wearable sensor devices in different areas. It has identified that IoT is widely used in healthcare but presents numerous privacy and security challenges, as well as other options, as discussed in the results.

The key findings of this paper are as below:

Unresolved security areas in WWSNs include third-party sharing, weak policies, handling extensive data, the increasing use of interconnected wireless devices, and a lack of understanding in managing health data with WWSN in IoT, fog computing, cloud computing, and WBAN technologies. While blockchain technology is promising, it still needs to evolve its capacity to be more useful in the healthcare sector regarding third-party sharing and warding off cyber-attacks. Additionally, wireless connectivity solutions must be more vital to provide end-to-end security due to the limited resources as malicious attacks are increasing in the healthcare sector, which must be addressed.

These findings benefit healthcare professionals and WWSN users by understanding the risks of using the wearable sensor device while managing health data by:

- Identifying the privacy and security challenges involved in WWSNs;
- Examining unresolved areas of security challenges in IoT, which need constant review;
- Considering blockchain technology in healthcare and concluding that it needs to be more mature to address security challenges;
- Examining the privacy and security challenges in wireless connection due to the limited resources used for remote sharing;

- Identifying the growing malicious attacks in healthcare every year as intruders mainly target health data;

Future reviews will focus on unresolved areas to provide solutions and recommend reviewing weak areas to propose better solutions.

Conflict of interest

There is no conflict of interest for this study.

References

[1] D. Sathya and P. G. Kumar, “Secured remote health monitoring system,” *Health Technol. Lett.*, vol. 4, pp. 228–232, 2017. https://doi.org/10.1049/htl.2017.0033.

[2] Z. Mahmood, H. Ning, A. Ullah, and X. Yao, “Secure Authentication and Prescription Safety Protocol for Telecare Health Services Using Ubiquitous IoT,” *Appl. Sci.*, vol. 7, no. 1069, 2017. https://doi.org/10.3390/app7101069.

[3] Y. A. Alsahafi and V. Gay, “An overview of electronic personal health records,” *Health Policy Technol.*, vol. 7, pp. 427–432, 2018. https://doi.org/10.1016/j.hlpt.2018.10.004.

[4] T. Yaqoob, H. Abbas, and M. Atiquzzaman, “Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review,” *IEEE Commun. Surv. Tutor.*, vol. 21, pp. 3723–3768, 2019. https://doi.org/10.1109/COMST.2019.2914094.

[5] S. Banerjee, T. Hemphill, and P. Longstreet, “Wearable devices and healthcare: Data sharing and privacy,” *Inf. Soc.*, vol. 34, pp. 49–57, 2018. https://doi.org/10.1080/01972243.2017.1391912.

[6] J. B. Awotunde, R. G. Jimoh, S. O. Folorunso, E. A. Adeniyi, K. M. Abiodun, and O. O. Banjo, “Privacy and security concerns in IoT-based healthcare systems,” in *The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care*, Cham, Switzerland: Springer, 2021, pp. 105–134. https://doi.org/10.1007/978-3-030-75220-0_6.

[7] Z. A. Solangi, Y. A. Solangi, S. Chandio, M. S. bin Hamzah, and A. Shah, “The future of data privacy and security concerns in Internet of Things,” in *Proc. 2018 IEEE Int. Conf. Innovative Res. Dev.*, Bangkok, Thailand, May 11–12, 2018. https://doi.org/10.1109/ICIRD.2018.8376320.

[8] A. Bajaj, M. Bhatnagar, and A. Chauhan, “Recent trends in internet of medical things: a review,” in *Advances in Machine Learning and Computational Intelligence*, Singapore: Springer, 2021, pp. 645–656. https://doi.org/10.1007/978-981-15-5243-4_61.

[9] S. D. Mamdiwar, Z. Shakruwala, U. Chadha, K. Srinivasan, and C.-Y. Chang, “Recent Advances on IoT-Assisted Wearable Sensor Systems for Healthcare Monitoring,” *Biosensors*, vol. 11, no. 372, 2021. https://doi.org/10.3390/bios11100372.

[10] “HEIR innovations for healthcare systems,” Accessed: Jan. 4, 2021. [Online]. Available: https://heir2020.eu/sites/default/files/docs/HEIR_D1.1_HEIR%20Innovations_V1.0.pdf.

[11] S.-D. Bao, M. Chen, and G.-Z. Yang, “A Method of Signal Scrambling to Secure Data Storage for Healthcare Applications,” *IEEE J. Biomed. Health Inform.*, vol. 21, pp. 1487–1494, 2017. https://doi.org/10.1109/jbhi.2017.2679979.

[12] M. Al-Zinati, T. Almasri, M. Alsmirat, and Y. Jararweh, “Enabling multiple health security threats detection using mobile edge computing,” *Simul. Model. Pr. Theory*, vol. 101, no. 101957, 2020. https://doi.org/10.1016/j.simpat.2019.101957.

[13] H. Wang, J. Ning, X. Huang, G. Wei, G. S. Poh, and X. Liu, “Secure Fine-grained Encrypted Keyword Search for e-Healthcare Cloud,” *IEEE Trans. Dependable Secur. Comput.*, vol. 18, pp. 1307–1319, 2019. https://doi.org/10.1109/tdsc.2019.2916569.

[14] Z. Shahbazi and Y.-C. Byun, “Towards a Secure Thermal-Energy Aware Routing Protocol in Wireless Body Area Network Based on Blockchain Technology,” *Sensors*, vol. 20, no. 3604, 2020. https://doi.org/10.3390/s20123604.

[15] L. Cilliers, “Wearable devices in healthcare: Privacy and information security issues,” *Health Inf. Manag. J.*, vol. 49, pp. 150–156, 2019. https://doi.org/10.1177/1833358319851684.

[16] K. T. Shah, “Privacy and security issues of wearables in healthcare,” M.S. thesis, Flind. Univ., Adelaide, Australia, Jun. 2019.

[17] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, “HealthBlock: A secure blockchain-based healthcare data management system,” *Comput. Netw.*, vol. 200, p. 108500, 2021. https://doi.org/10.1016/j.comnet.2021.108500.

[18] V. Kapoor, R. Singh, R. Reddy, and P. Churi, “Privacy issues in wearable technology: An intrinsic review,” in *Proc. Int. Conf. Innovative Computing & Commun. (ICICC)*, Delhi, India, Feb. 21–23, 2020. http://dx.doi.org/10.2139/ssrn.3566918.

[19] A. Kumar, K. Singh, T. Khan, A. Ahmadian, M. H. M. Saad, and M. Manjul, “ETAS: An Efficient Trust Assessment Scheme for BANs,” *IEEE Access*, vol. 9, pp. 83214–83233, 2021. https://doi.org/10.1109/access.2021.3086534.

[20] V. Chang, L. M. T. Doan, Q. A. Xu, K. Hall, Y. A. Wang, and M. M. Kamal, “Digitalization in omnichannel healthcare supply chain businesses: The role of smart wearable devices,” *J. Bus. Res.*, vol. 156, 2023. https://doi.org/10.1016/j.jbusres.2022.113369.

[21] H. H. Alshammari, “The internet of things healthcare monitoring system based on MQTT protocol,” *Alex. Eng. J.*, vol. 69, pp. 275–287, 2023. https://doi.org/10.1016/j.aej.2023.01.065.

[22] A. L. Martínez, M. Gil Pérez, and A. Ruiz-Martínez, “A Comprehensive Review of the State-of-the-Art on Security and Privacy Issues in Healthcare,” *ACM Comput. Surv.*, vol. 55, pp. 1–38, 2023. https://doi.org/10.1145/3571156.

[23] S. Tanwar, S. Badotra, M. Gupta, and A. Rana, “Efficient and secure multiple digital signature to prevent forgery based on ECC,” *Int. J. Appl. Sci. Eng.*, vol. 18, pp. 1–7, 2021. https://doi.org/10.6703/ijase.202109_18(5).010.

[24] A. Almalawi, A. I. Khan, F. Alsolami, Y. B. Abushark, and A. S. Alfakeeh, “Managing Security of Healthcare Data for a Modern Healthcare System,” *Sensors*, vol. 23, no. 3612, 2023. https://doi.org/10.3390/s23073612.

[25] B. B. Mcshane and U. Böckenholt, “Single-Paper Meta-Analysis: Benefits for Study Summary, Theory Testing, and Replicability,” *J. Consum. Res.*, vol. 43, pp. 1048–1063, 2017. https://doi.org/10.1093/jcr/ucw085.

[26] M. Crowther, W. Lim, and M. A. Crowther, “Systematic review and meta-analysis methodology,” *Blood*, vol. 116, pp. 3140–3146, 2010. https://doi.org/10.1182/blood-2010-05-280883.

[27] L. Aversano, M. L. Bernardi, M. Cimitile, and R. Pecori, “A systematic review on Deep Learning approaches for IoT security,” *Comput. Sci. Rev.*, vol. 40, p. 100389, 2021. https://doi.org/10.1016/j.cosrev.2021.100389.

[28] J. Passos, et al., “Wearables and Internet of Things (IoT) Technologies for Fitness Assessment: A Systematic Review,” *Sensors*, vol. 21, no. 5418, 2021. https://doi.org/10.3390/s21165418.

[29] M. S. Anker, S. Hadzibegovic, A. Lena, and W. Haverkamp, “The difference in referencing in Web of Science, Scopus, and Google Scholar,” *ESC Hear. Fail.*, vol. 6, pp. 1291–1312, 2019. https://doi.org/10.1002/ehf2.12583.

[30] S. Rajeswari and K. Praveena, “Analysis of ‘Big Data’ Research Output in IEEExplore: A Bibliometric Study,” *Libr. Philos. Pract.*, pp. 1–11, 2021.

[31] A. H. M. Aman, W. H. Hassan, S. Sameen, Z. S. Attarbashi, M. Alizadeh, and L. A. Latiff, “IoMT amid COVID-19 pandemic: Application, architecture, technology, and security,” *J. Netw. Comput. Appl.*, vol. 174, p. 102886, 2021. https://doi.org/10.1016/j.jnca.2020.102886.

[32] Z. Ashfaq, et al., “A review of enabling technologies for Internet of Medical Things (IoMT) Ecosystem,” *Ain Shams Eng. J.*, vol. 13, 2022. https://doi.org/10.1016/j.asej.2021.101660.

[33] N. L. Amah, “Fundamental Security Challenges in Internet of Things Healthcare Services,” Accessed: Mar. 24, 2017. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386210.

[34] A. E. Omolara, et al., “The internet of things security: A survey encompassing unexplored areas and new insights,” *Comput. Secur.*, vol. 112, p. 102494, 2021. https://doi.org/10.1016/j.cose.2021.102494.

[35] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, “Security and Privacy in the Medical Internet of Things: A Review,” *Secur. Commun. Netw.*, vol. 2018, pp. 1–9, 2018. https://doi.org/10.1155/2018/5978636.

[36] X. Li, H.-N. Dai, Q. Wang, M. Imran, D. Li, and M. A. Imran, “Securing Internet of Medical Things with Friendly-jamming schemes,” *Comput. Commun.*, vol. 160, pp. 431–442, 2020. https://doi.org/10.1016/j.comcom.2020.06.026.

[37] S. Alam, et al., “Blockchain-Based Solutions Supporting Reliable Healthcare for Fog Computing and Internet of Medical Things (IoMT) Integration,” *Sustainability*, vol. 14, no. 15312, 2022. https://doi.org/10.3390/su142215312.

[38] M. M. Dhanvijay and S. C. Patil, “Internet of Things: A survey of enabling technologies in healthcare and its applications,” *Comput. Netw.*, vol. 153, pp. 113–131, 2019. https://doi.org/10.1016/j.comnet.2019.03.006.

[39] K. Kakhi, R. Alizadehsani, H. D. Kabir, A. Khosravi, S. Nahavandi, and U. R. Acharya, “The internet of medical things and artificial intelligence: trends, challenges, and opportunities,” *Biocybern. Biomed. Eng.*, vol. 42, pp. 749–771, 2022. https://doi.org/10.1016/j.bbe.2022.05.008.

[40] A. Motwani, P. K. Shukla, and M. Pawar, “Ubiquitous and smart healthcare monitoring frameworks based on machine learning: A comprehensive review,” *Artif. Intell. Med.*, vol. 134, p. 102431, 2022. https://doi.org/10.1016/j.artmed.2022.102431.

[41] A. Hemmati and A. M. Rahmani, “Internet of Medical Things in the COVID-19 Era: A Systematic Literature Review,” *Sustainability*, vol. 14, p. 12637, 2022. https://doi.org/10.3390/su141912637.

[42] T. Shakeel, et al., “A survey on COVID-19 impact in the healthcare domain: worldwide market implementation, applications, security and privacy issues, challenges and future prospects,” *Complex Intell. Syst.*, vol. 9, pp. 1027–1058, 2023. https://doi.org/10.1007/s40747-022-00767-w.

[43] G. Aceto, V. Persico, and A. Pescapé, “The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges,” *J. Netw. Comput. Appl.*, vol. 107, pp. 125–154, 2018. https://doi.org/10.1016/j.jnca.2018.02.008.

[44] K. Pavithr, and G. Saravanan, “IoT, an Emerging Technology for Next Generation Medical Devices in Support of Cardiac Health Care—A Comprehensive Review,” *Int. Res. J. Multidiscip. Technovation*, vol. 1, pp. 35–40, 2019. https://doi.org/10.34256/irjmtcon5.

[45] M. Younan, E. H. Houssein, M. Elhoseny, and A. A. Ali, “Challenges and recommended technologies for the industrial internet of things: A comprehensive review,” *Measurement*, vol. 151, p. 107198, 2020. https://doi.org/10.1016/j.measurement.2019.107198.

[46] Z. Iftikhar, et al., “Privacy Preservation in Resource-Constrained IoT Devices Using Blockchain—A Survey,” *Electronics*, vol. 10, p. 1732, 2021. https://doi.org/10.3390/electronics10141732.

[47] S. Sengupta, “A Secured Biometric-Based Authentication Scheme in IoT-Based Patient Monitoring System,” in *Emerging Technology in Modelling and Graphics*, Singapore: Springer, 2020, pp. 501–518. https://doi.org/10.1007/978-981-13-7403-6_44.

[48] M. Aly, F. Khomh, M. Haoues, A. Quintero, and S. Yacout, “Enforcing security in Internet of Things frameworks: A Systematic Literature Review,” *Internet Things*, vol. 6, p. 100050, 2019. https://doi.org/10.1016/j.iot.2019.100050.

[49] A. I. Awad, M. M. Fouda, M. M. Khashaba, E. R. Mohamed, and K. M. Hosny, “Utilization of mobile edge computing on the Internet of Medical Things: A survey,” *ICT Express*, vol. 9, pp. 473–485, 2023. https://doi.org/10.1016/j.icte.2022.05.006.

[50] A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, “A survey on the adoption of blockchain in IoT: challenges and solutions,” *Blockchain: Res. Appl.*, vol. 2, p. 100006, 2021. https://doi.org/10.1016/j.bcra.2021.100006.

[51] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, “A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions,” *Electronics*, vol. 9, p. 1177, 2020. https://doi.org/10.3390/electronics9071177.

[52] S. Hamdan, M. Ayyash, and S. Almajali, “Edge-Computing Architectures for Internet of Things Applications: A Survey,” *Sensors*, vol. 20, no. 6441, 2020. https://doi.org/10.3390/s20226441.

[53] J. Ghosh, G. Samanta, and C. Chakraborty, “Smart health care for societies: An insight into the implantable and wearable devices for remote health monitoring,” in *Green Technological Innovation for Sustainable Smart Societies*, Cham, Switzerland: Springer, 2021, pp. 89–113. https://doi.org/10.1007/978-3-030-73295-0_5.

[54] G. Bigini, V. Freschi, and E. Lattanzi, “A Review on Blockchain for the Internet of Medical Things: Definitions, Challenges, Applications, and Vision,” *Futur. Internet*, vol. 12, p. 208, 2020. https://doi.org/10.3390/fi12120208.

[55] A. J. Perez and S. Zeadally, “Privacy Issues and Solutions for Consumer Wearables,” *IT Prof.*, vol. 20, pp. 46–56, 2017. https://doi.org/10.1109/mitp.2017.265105905.

[56] D. Bhushan and R. Agrawal, “Security Challenges for Designing Wearable and IoT Solutions,” in *A Handbook of Internet of Things in Biomedical and Cyber Physical System*, Cham, Switzerland: Springer, 2020, pp. 109–138. https://doi.org/10.1007/978-3-030-23983-1_5.

[57] S. Abdulmalek, et al., “IoT-Based Healthcare-Monitoring System towards Improving Quality of Life: A Review,” *Healthcare*, vol. 10, p. 1993, 2022. https://doi.org/10.3390/healthcare10101993.

[58] A. Alabdulatif, I. Khalil, and M. S. Rahman, “Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis,” *Appl. Sci.*, vol. 12, p. 11039, 2022. https://doi.org/10.3390/app122111039.

[59] P. K. R. Maddikunta, et al., “Incentive techniques for the Internet of Things: A survey,” *J. Netw. Comput. Appl.*, vol. 206, 2022. https://doi.org/10.1016/j.jnca.2022.103464.

[60] Z. Ahmadi, M. H. Kashani, M. Nikravan, and E. Mahdipour, “Fog-based healthcare systems: A systematic review,” *Multimedia Tools Appl.*, vol. 80, pp. 36361–36400, 2021. https://doi.org/10.1007/s11042-021-11227-x.

[61] J. Singh, P. Singh, and S. S. Gill, "Fog computing: A taxonomy, systematic review, current trends and research challenges," *J. Parallel Distrib. Comput.*, vol. 157, pp. 56–85, 2021. https://doi.org/10.1016/j.jpdc.2021.06.005.

[62] M. Azees, P. Vijayakumar, M. Karuppiah, and A. Nayyar, "An efficient anonymous authentication and confidentiality preservation schemes for secure communications in wireless body area networks," *Wirel. Netw.*, vol. 27, pp. 2119–2130, 2021. https://doi.org/10.1007/s11276-021-02560-y.

[63] S. Kumar, A. S. Tomar, and S. K. Chaurasiya, "Enhanced secure transmission of data in WBAN with predictive model for health care applications," *Intell. Decis. Technol.*, vol. 13, pp. 211–218, 2019. https://doi.org/10.3233/IDT-170182.

[64] K. Hasan, K. Biswas, K. Ahmed, N. S. Nafi, and S. Islam, "A comprehensive review of wireless body area network," *J. Netw. Comput. Appl.*, vol. 143, pp. 178–198, 2019. https://doi.org/10.1016/j.jnca.2019.06.016.

[65] J. V. Ananthi and P. S. H. Jose, "A Perspective Review of Security Challenges in Body Area Networks for Healthcare Applications," *Int. J. Wirel. Inf. Netw.*, vol. 28, pp. 451–466, 2021. https://doi.org/10.1007/s10776-021-00538-3.

[66] Z. Xu, C. Xu, H. Chen, and F. Yang, "A lightweight anonymous mutual authentication and key agreement scheme for WBAN," *Concurr. Comput. Pr. Exp.*, vol. 31, 2019. https://doi.org/10.1002/cpe.5295.

[67] V. Bhuse and H. Sinha, "Secure application for health monitoring," in *Proc. Eur. Conf. Inf. Warfare Secur. (ECCWS 2019)*, Coimbra, Portugal, Jul. 4–5, 2019, pp. 31–36.

[68] K. Azbeg, O. Ouchetto, S. Andaloussi, and L. Fetjah, "A Taxonomic Review of the Use of IoT and Blockchain in Healthcare Applications," *IRBM*, vol. 43, pp. 511–519, 2022. https://doi.org/10.1016/j.irbm.2021.05.003.

[69] A. S. Mahmoud and N. M. Mahmood, "A secure biomedical data sharing framework based on mCloud," *Int. J. Nonlinear Anal. Appl.*, vol. 12, pp. 1659–1671, 2021. https://doi.org/10.22075/ijnaa.2021.5295.

[70] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A Decentralized Privacy-Preserving Healthcare Blockchain for IoT," *Sensors*, vol. 19, p. 326, 2019. https://doi.org/10.3390/s19020326.

[71] M. Nikooghadam, H. Amintoosi, and S. Kumari, "On the Security of 'Secure and Lightweight Authentication with Key Agreement for Smart Wearable Systems'," *Wirel. Pers. Commun.*, vol. 120, pp. 1–8, 2021. https://doi.org/10.1007/s11277-021-08430-2.

[72] P. L. Rini, "Secure and Privacy Based Home Patient Monitoring Internet of Things (HPMIoT)," in *Advances in Parallel Computing Technologies and Applications*, Amsterdam, The Netherlands: IOS Press, 2021, pp. 55–62.

[73] D. D. Taralunga and B. C. Florea, "A Blockchain-Enabled Framework for mHealth Systems," *Sensors*, vol. 21, p. 2828, 2021. https://doi.org/10.3390/s21082828.

[74] L. Hong, M. Luo, R. Wang, P. Lu, W. Lu, and L. Lu, "Big Data in Health Care: Applications and Challenges," *Data Inf. Manag.*, 2019. https://doi.org/10.2478/dim-2018-00014.

[75] J. L. Shah, H. F. Bhat, and A. I. Khan, "CloudIoT-Driven Healthcare: Review, Architecture, Security Implications, and Open Research Issues," in *Advanced Healthcare Systems: Empowering Physicians with IoT-Enabled Technologies*, Hoboken, NJ, USA: Wiley, 2022, pp. 173–253. https://doi.org/10.1002/9781119769293.ch11.

[76] F. Al-Turjman, "Intelligence and security in big 5G-oriented IoNT: An overview," *Futur. Gener. Comput. Syst.*, vol. 102, pp. 357–368, 2019. https://doi.org/10.1016/j.future.2019.08.009.

[77] F. Pervez, J. Qadir, M. Khalil, T. Yaqoob, U. Ashraf, and S. Younis, "Wireless Technologies for Emergency Response: A Comprehensive Review and Some Guidelines," *IEEE Access*, vol. 6, pp. 71814–71838, 2018. https://doi.org/10.1109/access.2018.2878898.

[78] C. O. Alenoghena, et al., "eHealth: A Survey of Architectures, Developments in mHealth, Security Concerns and Solutions," *Int. J. Environ. Res. Public Health*, vol. 19, p. 13071, 2022. https://doi.org/10.3390/ijerph192013071.

[79] S. Chaudhary, et al., "A Taxonomy on Smart Healthcare Technologies: Security Framework, Case Study, and Future Directions," *J. Sens.*, vol. 2022, pp. 1–30, 2022. https://doi.org/10.1155/2022/1863838.

[80] R. Talati and P. Chaudhari, "The Road-ahead for E-healthcare 4.0: A Review of Security Challenges," in *Proc. 1st Int. Conf. Inform. (ICI)*, Noida, India, Apr. 14–16, 2022. https://doi.org/10.1109/ICI53355.2022.9786917.

[81] S. B. Junaid, et al., "Recent Advancements in Emerging Technologies for Healthcare Management Systems: A Survey," *Healthcare*, vol. 10, p. 1940, 2022. https://doi.org/10.3390/healthcare10101940.

[82] S. Apte, et al., "Biomechanical Response of the Lower Extremity to Running-Induced Acute Fatigue: A Systematic Review," *Front. Physiol.*, vol. 12, 2021. https://doi.org/10.3389/fphys.2021.646042.

[83] B. A. Ojokoh, et al., "Contact Tracing Strategies for COVID-19 Prevention and Containment: A Scoping Review," *Big Data Cogn. Comput.*, vol. 6, p. 111, 2022. https://doi.org/10.3390/bdcc6040111.

[84] M. Saifuzzaman, T. N. Ananna, M. J. M. Chowdhury, S. Ferdous, and F. Chowdhury, "A systematic literature review on wearable health data publishing under differential privacy," *Int. J. Inf. Secur.*, vol. 21, pp. 847–872, 2022. https://doi.org/10.1007/s10207-021-00576-1.

[85] Z. Lin, et al., "Pain Without Gain: Destructive Beamforming from a Malicious RIS Perspective in IoT Networks," *IEEE Internet Things J.*, vol. 11, pp. 7619–7629, 2023. https://doi.org/10.1109/jiot.2023.3316830.

[86] H. Mahmud and T. Rahman, "An Application of blockchain to securely acquire, diagnose and share clinical data through smartphone," *Peer-to-Peer Netw. Appl.*, vol. 14, pp. 3758–3777, 2021. https://doi.org/10.1007/s12083-021-01210-6.

[87] J. Ormanis and K. Nesenbergs, "Human skin as data transmission medium for improved privacy and usability in wearable electronics," in *Proc. 2018 IEEE Int. Symp. Med. Meas. Appl. (MeMeA)*, Rome, Italy, Jun. 11–13, 2018. https://doi.org/10.1109/MeMeA.2018.8438754.

[88] D. C. Nguyen, et al., "Federated Learning Meets Blockchain in Edge Computing: Opportunities and Challenges," *IEEE Internet Things J.*, vol. 8, pp. 12806–12825, 2021. https://doi.org/10.1109/jiot.2021.3072611.

[89] G. Zhuo and H. Yang, "Privacy-preserving context-aware friend discovery based on mobile sensing," in *Proc. 2018 IEEE Int. Conf. Consum. Electron. (ICCE)*, Las Vegas, NV, USA, Jan. 12–14, 2018. https://doi.org/10.1109/ICCE.2018.8326325.

[90] O. B. Ohwo and A. D. Olujimi, "A Comparative Review of Emerging Wireless Technology," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Syst.*, vol. 7, pp. 163–175, 2020.

[91] H. K. Bharadwaj, et al., "A Review on the Role of Machine Learning in Enabling IoT Based Healthcare Applications," *IEEE Access*, vol. 9, pp. 38859–38890, 2021. https://doi.org/10.1109/access.2021.3059858.

[92] V. Vijayan, J. P. Connolly, J. Condell, N. McKelvey, and P. Gardiner, "Review of Wearable Devices and Data Collection Considerations for Connected Health," *Sensors*, vol. 21, p. 5589, 2021. https://doi.org/10.3390/s21165589.

[93] L. Deng, Y. Yang, and R. Gao, "Certificateless Designated Verifier Anonymous Aggregate Signature Scheme for Healthcare Wireless Sensor Networks," *IEEE Internet Things J.*, vol. 8, pp. 8897–8909, 2021. https://doi.org/10.1109/jiot.2021.3056097.

[94] I. A. Sawaneh, I. Sankoh, and D. K. Koroma, "A survey on security issues and wearable sensors in wireless body area network for healthcare system," in *Proc. 14th Int. Comput. Conf. Wavelet Active Media Technol. Inform. Process. (ICCWAMTIP)*, Chengdu, China, Dec. 15–17, 2017. https://doi.org/10.1109/ICCWAMTIP.2017.8301502.

[95] M. A. Khan, M. T. Quasim, N. S. Alghamdi, and M. Y. Khan, "A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data," *IEEE Access*, vol. 8, pp. 52018–52027, 2020. https://doi.org/10.1109/ACCESS.2020.2980739.

[96] A. Darwish and A. E. Hassanien, "Cyber physical systems design, methodology, and integration: the current status and future outlook," *J. Ambient Intell. Humaniz. Comput.*, vol. 9, pp. 1541–1556, 2017. https://doi.org/10.1007/s12652-017-0575-4.

[97] A. Cernian, B. Tiganoaia, I. Sacala, A. Pavel, and A. Iftemi, "PatientDataChain: A Blockchain-Based Approach to Integrate Personal Health Records," *Sensors*, vol. 20, p. 6538, 2020. https://doi.org/10.3390/s20226538.

[98] M. Nikooghadam, H. Amintoosi, and N. Bagheri, "Lightweight authentication for remote healthcare systems in cloud-IoT," in *Proc. 10th Int. Conf. Comput. Knowl. Eng. (ICCKE)*, Mashhad, Iran, Oct. 29–30, 2020. https://doi.org/10.1109/ICCKE50421.2020.9303671.

[99] A. Vazirani, O. O'Donoghue, D. Brindley, and E. Meinert, "Implementing Blockchains for Efficient Health Care: Systematic Review," *J. Med Internet Res.*, vol. 21, e12439, 2019. https://doi.org/10.2196/12439.

[100] S. A. Shah and F. Fioranelli, "RF Sensing Technologies for Assisted Daily Living in Healthcare: A Comprehensive Review," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 34, pp. 26–44, 2019. https://doi.org/10.1109/maes.2019.2933971.

[101] H. Tahir, R. Tahir, and K. McDonald-Maier, "On the security of consumer wearable devices in the Internet of Things," *PLoS ONE*, vol. 13, e0195487, 2018. https://doi.org/10.1371/journal.pone.0195487.

[102] T. Handel, M. Schreiber, K. Rothmaler, and G. Ivanova, "Data security and raw data access of contemporary mobile sensor devices," in *World Congress on Medical Physics and Biomedical Engineering 2018*, Singapore: Springer, 2019, pp. 397–400. https://doi.org/10.1007/978-981-10-9035-6_73.

[103] A. Vaniprabha and P. Poongodi, "Augmented lightweight security scheme with access control model for wireless medical sensor networks," *Clust. Comput.*, vol. 22, pp. 12495–12505, 2018. https://doi.org/10.1007/s10586-017-1669-7.

[104] M. Abubakar, Z. Jaroucheh, A. Al Dubai, and B. Buchanan, “A Decentralised Authentication and Access Control Mechanism for Medical Wearable Sensors Data,” in *Proc. 2021 IEEE Int. Conf. Omni-Layer Intell. Syst. (COINS)*, Barcelona, Spain, Aug. 23–25, 2021. https://doi.org/10.1109/COINS51742.2021.9524172.

[105] A. Adam, A. Abubakar, and M. Mahmud, “Sensor Enhanced Health Information Systems: Issues and Challenges,” *Int. J. Interact. Mob. Technol. (iJIM)*, vol. 13, pp. 99–114, 2019. https://doi.org/10.3991/ijim.v13i01.7037.

[106] A. H. Seh, et al., “Healthcare Data Breaches: Insights and Implications,” *Healthcare*, vol. 8, p. 133, 2020. https://doi.org/10.3390/healthcare8020133.

[107] R. A. Tariq and P. B. Hackert, “Patient Confidentiality: StatPearls,” Accessed: Aug. 24, 2018. [Online]. Available: https://europepmc.org/article/MED/30137825.

[108] A. Rejeb, et al., “Unleashing the power of internet of things and blockchain: A comprehensive analysis and future directions,” *Internet Things Cyber-Physical Syst.*, vol. 4, pp. 1–18, 2024. https://doi.org/10.1016/j.iotcps.2023.06.003.

[109] H. A. Al-Ghuraybi, M. A. AlZain, and B. Soh, “Exploring the integration of blockchain technology, physical unclonable function, and machine learning for authentication in cyber-physical systems,” *Multimedia Tools Appl.*, pp. 1–44, 2023. https://doi.org/10.1007/s11042-023-16979-2.

[110] N. Li, et al., “A review of security issues and solutions for precision health in Internet-of-Medical-Things systems,” *Secur. Saf.*, vol. 2, 2023. https://doi.org/10.1051/sands/2022010.

[111] M. Shafay, R. W. Ahmad, K. Salah, I. Yaqoob, R. Jayaraman, and M. Omar, “Blockchain for deep learning: review and open challenges,” *Clust. Comput.*, vol. 26, pp. 197–221, 2022. https://doi.org/10.1007/s10586-022-03582-7.

[112] S. B. Weber, S. Stein, M. Pilgermann, and T. Schrader, “Attack Detection for Medical Cyber-Physical Systems–A Systematic Literature Review,” *IEEE Access*, vol. 11, pp. 41796–41815, 2023. https://doi.org/10.1109/access.2023.3270225.

[113] R. Kumar, S. K. Gupta, H.-C. Wang, C. S. Kumari, and S. S. V. P. Korlam, “From Efficiency to Sustainability: Exploring the Potential of 6G for a Greener Future,” *Sustainability*, vol. 15, p. 16387, 2023. https://doi.org/10.3390/su152316387.

[114] S. M. Rajagopal and R. Buyya, “FedSDM: Federated learning based smart decision making module for ECG data in IoT integrated Edge–Fog–Cloud computing environments,” *Internet Things*, vol. 22, 2023. https://doi.org/10.1016/j.iot.2023.100784.

[115] Z. Lin, M. Lin, T. de Cola, J.-B. Wang, W.-P. Zhu, and J. Cheng, “Supporting IoT With Rate-Splitting Multiple Access in Satellite and Aerial-Integrated Networks,” *IEEE Internet Things J.*, vol. 8, pp. 11123–11134, 2021. https://doi.org/10.1109/jiot.2021.3051603.

[116] Z. Lin, M. Lin, B. Champagne, W.-P. Zhu, and N. Al-Dhahir, “Secrecy-Energy Efficient Hybrid Beamforming for Satellite-Terrestrial Integrated Networks,” *IEEE Trans. Commun.*, vol. 69, pp. 6345–6360, 2021. https://doi.org/10.1109/tcomm.2021.3088898.

[117] K. An, M. Lin, J. Ouyang, and W.-P. Zhu, “Secure Transmission in Cognitive Satellite Terrestrial Networks,” *IEEE J. Sel. Areas Commun.*, vol. 34, pp. 3025–3037, 2016. https://doi.org/10.1109/jsac.2016.2615261.

[118] B. Samhan, T. Crampton, and R. Ruane, “The Trajectory of IT in Healthcare at HICSS: A Literature Review, Analysis, and Future Directions,” *Commun. Assoc. Inf. Syst.*, vol. 43, pp. 792–845, 2018. https://doi.org/10.17705/1cais.04341.

[119] W. B. Millard, “Where bits and bytes meet flesh and blood: Hospital responses to malware attacks,” *Ann. Emerg. Med.*, vol. 70, pp. A17–A21, 2017.

[120] O. S. Albahri, et al., “Systematic Review of Real-time Remote Health Monitoring System in Triage and Priority-Based Sensor Technology: Taxonomy, Open Challenges, Motivation and Recommendations,” *J. Med Syst.*, vol. 42, p. 80, 2018. https://doi.org/10.1007/s10916-018-0943-4.

[121] J. Qi, P. Yang, A. Waraich, Z. Deng, Y. Zhao, and Y. Yang, “Examining sensor-based physical activity recognition and monitoring for healthcare using Internet of Things: A systematic review,” *J. Biomed. Inform.*, vol. 87, pp. 138–153, 2018. https://doi.org/10.1016/j.jbi.2018.09.002.

[122] M. Gochoo, F. Alnajjar, T.-H. Tan, and S. Khalid, “Towards Privacy-Preserved Aging in Place: A Systematic Review,” *Sensors*, vol. 21, p. 3082, 2021. https://doi.org/10.3390/s21093082.

[123] A. I. Alsalibi, M. K. Y. Shambour, M. A. Abu-Hashem, M. Shehab, and Q. Shambour, “Internet of Things in Health Care: A Survey,” in *Hybrid Artificial Intelligence and IoT in Healthcare*, Singapore: Springer, 2021, pp. 165–200. https://doi.org/10.1007/978-981-16-2972-3_9.