Journal of
Sensor and Actuator Networks

MDPI

Review

A Systematic Review of Radio Frequency Threats in IoMT

Irrai Anbu Jayaraj [1], Bharanidharan Shanmugam [1,*], Sami Azam [2] and Ganthan Narayana Samy [3]

[1] Energy and Resources Institute, College of Engineering, IT and Environment, Charles Darwin University, Darwin, NT 0909, Australia
[2] College of Engineering, IT and Environment, Charles Darwin University, Darwin, NT 0909, Australia
[3] Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Kuala Lumpur 54100, Malaysia
* Correspondence: bharanidharan.shanmugam@cdu.edu.au

Abstract: In evolving technology, attacks on medical devices are optimized due to the driving force of AI, computer vision, mixed reality, and the internet of things (IoT). Optimizing cybersecurity on the internet of medical things (IoMT) and building cyber resiliency against crime-as-a-service (CaaS) in the healthcare ecosystem are challenging due to various attacks, including spectrum-level threats at the physical layer. Therefore, we conducted a systematic literature review to identify the research gaps and propose potential solutions to spectrum threats on IoMT devices. The purpose of this study is to provide an overview of the literature on wireless spectrum attacks. The papers we reviewed covered cyber impacts, layered attacks, attacks on protocols, sniffing attacks, field experimentation with cybersecurity testbeds, radiofrequency machine learning, and data collection. In the final section, we discuss future directions, including the sniffing attack mitigation framework in IoMT devices operating under a machine implantable communication system (MICS). To analyze the research papers about physical attacks against IoT in health care, we followed the Preferred Reporting Items for Systematic Reviews (PRISMA) guidelines. Scopus, PubMed, and Web of Science were searched for peer-reviewed articles, and we conducted a thorough search using these resources. The search on Scopus containing the terms "jamming attack" and "health" yielded 330 rows, and the investigation on WoS yielded 17 rows. The search terms "replay attack" and "health" yielded 372 rows in Scopus, while PubMed yielded 23 rows, and WoS yielded 50 articles. The search terms "side-channel attack" and "health" yielded 447 rows in Scopus, WoS yielded 30 articles, and the search terms "sniffing attack" and "health" yielded 18 rows in Scopus, while PubMed yielded 1 row, and WoS yielded 0 articles. The terms "spoofing attack" and "health" yielded 316 rows in Scopus, while PubMed yielded 5 rows, and WoS yielded 23 articles. Finally, the search terms "tampering attack" and "health" yielded 25 rows in Scopus, PubMed yielded 14 rows, and WoS yielded 46 rows. The search time frame was from 2003 to June 2022. The findings show a research gap in sniffing, tampering, and replay attacks on the IoMT. We have listed the items that were included and excluded and provided a detailed summary of SLR. A thorough analysis of potential gaps has been identified, and the results are visualized for ease of understanding.

Keywords: cybersecurity; health care; systematic review; internet of medical things; sniffing attacks; radiofrequency attacks

Citation: Jayaraj, I.A.; Shanmugam, B.; Azam, S.; Samy, G.N. A Systematic Review of Radio Frequency Threats in IoMT. *J. Sens. Actuator Netw.* **2022**, *11*, 62. https://doi.org/10.3390/jsan11040062

Academic Editor: Mohamed Amine Ferrag

Received: 17 August 2022
Accepted: 7 September 2022
Published: 28 September 2022

1. Introduction

Digital health is a promising platform to increase life expectancy and overcome the challenges that healthcare technologists must deal with. Among the promising research fields of today, the IoMT (internet of medical things)-based AR/VR (augmented reality/virtual reality) technologies strongly focus on the medical education and patient engagement areas of the healthcare ecosystem. However, digital transformation vulnerabilities are providing an opportunity to adversaries to explore less studied and little-known physical emanation attacks, including radio frequency, acoustic, ultrasonic, magnetic, photonic, seismic, infrared, electromagnetic, magnetic field temperature, and low-level vibration attacks

on air gap and non-air gap source systems [1–4]. To protect high- and low-value assets, there is a need to provide physical security between personal medical devices, healthcare providers, education, and patient-centric approaches. Additionally, the evolving nature of IoT-based healthcare ecosystems requires sound medical and ethical policies to ensure cybersecurity is safe and attack-aware. Because of disruptive technologies' demanding nature and the need to accelerate the learning curve of the workforce, the IoMT sector is growing more rapidly than ever, bringing new risks and vulnerabilities. The present-day wireless attacks are not limited to NFC (near field communication) [5], (BLE) bluetooth low energy [6], LTE (long-term evolution) [7], RF (radio frequency) [8], Wi-Fi (wireless fidelity), GPS (global positioning satellite), or SATCOM (satellite communications) but extend to other wireless spectrum technologies vulnerable to quality attribute attacks on reliability, safety, security, and integrity. In hospital settings, IoMT devices pose greater cyber risks than ever due to innovation in IoMT devices [8].

Table 1 shows RF attacks by the internet of things (IoT) layer and attack area description, and Figure 1 shows the wireless device, system, and communication technologies used in the healthcare ecosystem and threats by software-defined radio devices.

Table 1. RF attack by IoT layer and attack area description.

Type of Attack	IoT Layer	Attack Area Description
Primary emulation	Perception	The primary transmitter/antenna emits information or spilling of information.
Spectrum sensing	Perception	Fake identification and observation of spectrum sensing process.
Control channel attack	Network	Untrusted system or process collecting confidential information of trusted system/process.
Cross-layer attack	All layers	Parallel attack on all the layers of IoT.
SDR device attack	All layers	SDR device antenna/battery and other core part disruption.
Jamming attack	All layers	Decreasing signal to interference noise ratio by blocking the information transfer between transmitter and receiver in the communication channel.
Replay attack	All layers	Interception of signal between transmitter and receiver to accomplish fake transmission.
Sniffing attack	All layers	Closely monitoring the sensitive or unauthorized information between transmitter and receiver in the communication channel.
Tampering attack	All layers	Closely monitoring the sensitive or unauthorized information between transmitter and receiver in the communication channel and modification of process/parameters to compromise the system.
Denial attack	All layers	Closely monitoring the sensitive or unauthorized information between transmitter and receiver in the communication channel, modification of process/parameters, and disrupting the availability.

Hospital settings are vulnerable to various attacks, such as simulation and clone attacks in LFID (low-frequency identification), privacy leakage attacks (PLA) on contactless cards, replay and brute force attacks on pressure systems, sniffing and jamming attacks on Wi-Fi, the transmission of fake uplink data, and clone the tracker attacks and LTE sniffing attacks on mobiles. Information security incidents caused by intruders and unethical hackers are becoming more common, as evident from various research efforts on the IoT security and wireless sensor networks security and challenges, including medical devices and personal body area networks. Information spilling, session hijacking, and phishing attacks are frequent in healthcare infrastructure. Moreover, attack types based on the layer are becoming common in the hospital sector due to the low level of the cyber security maturity model, penetration testing to identify the vulnerabilities, and lack of cyber security awareness among business users and stakeholders.

Attack	Attack System	SDR device
Eavesdropping	ADS-B	RTL 2832U
	DECT	USRP N210 RTL2832U
	Near Field Communicatio..	USRP N210
GPS Spoofing	GNSS	USRP N210
IMSI catcher	GSM	USRP-N210/WBX USRP1
Jamming	OFDM	NI USRP 2921
Location leaks; denial of s..	LTE	USRP B210
Man in the middle	GSM	USRP B200
	IoT(Bluetooth 2.1)	USRP 2
Penetration Testing	Tactical Radio Networks	HackRF One
Protocols implementation	LoRaWan, BLE, IEEE802.1..	USRP E310
Replay	RFID	USRP N210/SBX
Side channel	Decryption AES-128 on 32..	USRP2,RTL 2832U
Spoofing	ACARS, FANS1/A	USRP B200
	Drones	USRP
	FM-based indoor localizat..	USRP B100/WBX
	Vehicular Security (TMPS ..	USRP N210/
TEMPEST	Computer display	PXI-e 5665 USRP N210/W..
vulnerabilities analysis on..	LTE	USRP N210

Attack
- Eavesdropping
- GPS Spoofing
- IMSI catcher
- Jamming
- Location leaks; denial of service
- Man in the middle
- Penetration Testing
- Protocols implementation
- Replay
- Side channel
- Spoofing
- TEMPEST
- vulnerabilities analysis on physical layer

Figure 1. Physical attack and attack system by SDR devices.

1.1. Radiofrequency Attacks

An RF attack is a type of hacking that does not require physical contact with the target. Electronic devices are disrupted, damaged, or interfered with by radio waves sent by the attacker. In addition to disrupting internet-connected devices, they can also affect computers, routers, printers, and other IoT devices. Software-defined radios (SDRs) are powerful tools for monitoring, intercepting, and manipulating digital communications. Additionally, they open the door to the internet of things. As SDRs become more prevalent, the threat of IoT hacks will increase. Figure 1 shows the possibilities of physical layer attacks and system attacks by SDR devices. As shown in Figure 1, spoofing, eavesdropping, and man-in-the-middle attacks have a combined 50% coverage when compared to the other attacks. Additionally, spoofing and eavesdropping are more significant than man-in-the-middle attacks in that range.

1.2. Recommended Solutions

There are still organizational, technological, and governance barriers that prevent the adoption of cybersecurity in healthcare IoT, but the coronavirus disease (COVID-19) pandemic has brought to light the need for a secure IoT to coordinate the transfer of confidential information, for temperature control of medical supplies and vaccines, radio frequency-based machine implantable communication systems, wearable technologies for remote patient monitoring, and patient-controlled drug delivery systems. The need to drive greater adoption of IoT security policies in healthcare cybersecurity makes it imperative to remove some of these barriers in concerted efforts to drive greater adoption. Although external factors such as COVID-19 alone may push the adoption of these technologies, such factors cannot achieve lasting and sustained effects [9].

We aimed to systematically review the IoMT to understand the research gap and identify RF hackers' locations. Our goal was to provide the healthcare community with better understanding, literacy, and appropriate advancements, as well as bring together IoMT and physical layer scientists. Additionally, we hope that this work will foster a greater interest in integrating IoMT systems into future healthcare applications and beyond. The following are the main contributions.

1. A description of the current state of research on internet of things (IoT) side-channel attacks.

2. The aim of this study was to understand the research gap about sniffing and replaying IoMT attacks in the healthcare ecosystem.
3. The research papers were reviewed top-down to facilitate our future research, including those on cybersecurity systems, cybersecurity frameworks, cyber-attacks on layers and protocols, radio frequency machine learning, and deep learning in a cybersecurity field experimentation.
4. The conclusions we have reached, and our plans for future work are presented.

In Table 2, cyber spectrum attacks are analyzed across journals. There is a lack of research on sniffing and tampering attacks, according to the results.

Table 2. Displays the search analysis of cyber spectrum attacks across journals.

Attack Search	Web of Science	Scopus	PubMed	Total
Jamming Attack	17	330	0	347
Replay Attack	50	372	23	445
Side-Channel Attack	30	447	0	477
Sniffing Attack	0	18	1	19
Spoofing Attack	23	316	5	344
Tampering Attack	25	46	14	85
Total	145	1529	43	1717

Our future research will be facilitated by reviewing research papers from the top down. Topics included systems for cybersecurity, cybersecurity frameworks, attacks on layers and protocols, radio frequency machine learning, and deep learning in the cybersecurity field. Table 3 shows the papers we reviewed.

Table 3. Summary of SLR.

Type of Attack	Section	Data	Method	Conclusion/Result
This framework provides details related to incident insights. It classifies incidents based on external, internal, and partner-based threats. It also provides insights into hacking evidence, including IoT forensics), malware behavior, social engineering attacks, privilege misuse, and known and unintentional errors.	3.1	2	3	The key metrics on incidents are classified based on victims (size of the organization), actors, actions, assets, attributes, timelines, impacts, and repeated events.
The research explains various attacks on that three-layer IoT architecture, starting with physical attacks, jamming attacks, relay attacks, Sybil, selective forwarding, side-channel, replay, evil twin, sniffing, and spoofing.	3.1	1	3	The paper shows goal-based classification and the evolving spectrum-level vulnerabilities causing significant disruption to the OSI.
Their investigation claims that mobilityand QoS will be high for specific communication protocols.	3.2	1	3	The reverse engineering of the spectrum to retrieve those payloads and understand the protocols becomes a base process of attack strategies. The hardness scale depends on the main contributing factors: encryption, frequency band, modulation, spread spectrum, and protocols.
How asset mobility contributes to the continuous evaluation and monitoring of high-value assets and elevates risk mitigation strategies and guidelines.	3.2	2	3	The paper evaluates the reasoning behind new cybersecurity threats from radio channel-based adversaries such as cluster drones, mobile networks, satellites, marine, aeronautical, in-depth space communication, and IoT.

Table 3. *Cont.*

Type of Attack	Section	Data	Method	Conclusion/Result
Categorization of attack levels—operating system level, user interface level—and how the sensitive information flows across the process are captured for further analysis.	3.3	2	3	The inheritance of password authentication shows the infancy of research rigor and does not contribute to sniffing attacks.
This paper contributes to knowledge more than the practical implementation of design, artifacts, proof of concepts, experimentation, evaluation, and future direction.	3.3	1	4	The main idea will enhance the motivation to identify the research focus with potential questions. IoMT is operating under MICS or ISM frequency.
The architectural design and completion of the Version 1 CASE-V testbed. They developed a web-based UI framework using the MEAN.	3.4	2	4	To reduce the dependability of an external penetration tester, a low-cost testbed can be performed to improve the effectiveness and usability of CSM.
The research claims that open-source hardware and software can develop a testbed within 500 euros for ethical Industrial Control System hacking, education, competency development, and research.	3.4	1	4	According to the analysis, insider threats and associated toolsimpact levels 0 and 1 compared to a remote intruder. The author's findings proved that a low-cost testbed is possible in the corporate ecosystem.
Overview of publicly available data sets for intelligent cybersecurity intrusion detection system. Also, it proposed how ML and DL techniques can be used to analyze the raw network traffic data having real-time traffics from APT, malware, and botnets.	3.5	2	4	The research investigated the pros and cons between Machine Learning (ML) and Deep Learning (DL) algorithm support vector machines (SVM), deep belief network (DBN), recursive neural network (RNN), convolutional neural network (CNN), Fast-RNN and difference between ML and DL in terms of data and hardware dependencies, Feature processing, problem solving and execution time.
They investigated the publicly available database—IEEE, Science Direct, ACM, and Springer Link, between 1990 and 2019 to address the questions.1.ML algorithm used for endpoint detection and response (EDR)2. Alternative available for the EDR.	3.5	2	4	The research claims to analyze the Publication Trends in EDR and the techniques used for EDR.
Literature review data = 1; Public dataset = 2.				Literature study = 3; Experimental Study = 4.

2. Methodology

In our systematic review [10], we have focused on the healthcare field, healthcare, and IoT, and the section starts with the research questions and the data sources. A detailed keyword search has been listed, followed by an analysis. VOS viewer has been utilized for visualization and has helped us identify critical research papers.

2.1. Research Questions

In this study, the following research questions were addressed [11]:

1. RQ1: How well has IoT been integrated into healthcare?
2. RQ2: What is the current state of healthcare-RF cybersecurity research?

2.2. The Source of Data

Three electronic databases were included in the systematic review:

- Web of Science (WoS);
- Scopus;

- PubMed.

The original research articles on IoT signal security in health care were identified using the Preferred Reporting Items for Systematic Reviews Meta-analysis (PRISMA) guidelines. Our search was for original research articles published exclusively in English between January 2002 and June 2022. This document contains PRISMA, as well as articles with full text and articles in English. We conducted a cross-disciplinary database search of research articles between inception and June 2022. To find articles published between 2012 and 2022, we used Boolean functions in electronic databases (PubMed, Scopus, and Web of Science).

In this section, we have reviewed the research papers related to the cybersecurity framework, the layered classification of IoT, and cybersecurity impacts. Then, we cascaded the studies on attacks on physical layer protocols and further reviewed radio frequency attacks (RFA) on the IoMT. For example, they were sniffing attacks, tampering attacks on vehicular sensors, and replay attacks. Our research studies use the PRISMA approach for the identification, screening, eligibility, and inclusion of research papers. Then, we used a systematic literature review (SLR) to identify papers contributing to our defined scope. Few studies and little-known information are available in the SLR approach on RF physical attacks on the IoMT and their analyzing trend through radio frequency machine learning (RFML) [12]. The core papers included in our research studies are directly associated with physical layer attacks. However, there are papers on IoT health care that provide industry and market acceptance from healthcare professionals [13]. We used the British Standards Institution [14] and the national initiative for cybersecurity careers and studies for our research [15]. The keywords are listed below.

2.3. Search Strategy and Selection Criteria

Following are the search strings we used to search Scopus, Web of Science, and PubMed:

ALL (“JAMMING ATTACK”) AND ALL (“HEALTH”) AND PUBYEAR > 2002

ALL (“REPLAY ATTACK”) AND ALL (“HEALTH”) AND PUBYEAR > 2002

ALL (“SNIFFING ATTACK”) AND ALL (“HEALTH”) AND PUBYEAR > 2002

ALL (“TAMPERING ATTACK”) AND ALL (“HEALTH”) ALL (“SIDE CHANNEL ATTACK”) AND ALL VAND PUBYEAR > 2002

ALL (“DENIAL ATTACK”) AND ALL (“HEALTH”) AND PUBYEAR > 2002

ALL (“SPOOFING”) AND ALL (“HEALTH”) AND PUBYEAR > 2002

The rejected keywords are “health care,” “physical attack,” “SDR,” “malicious,” “intruder,” and “adversaries.” In the last decade, there has been a significant positive increase in wireless security awareness and spectrum attack awareness. The research articles from the web of science (WOS), PubMed, and Scopus are included in our study. However, physical layer research contributions are relatively modest compared to other security layers. An article was excluded if it falls in another category other than cybersecurity physical layer attacks and health.

In June 2022, a search was conducted in the online digital libraries to locate the articles. An overview of the search and selection procedure is given in Figure 2 [16].

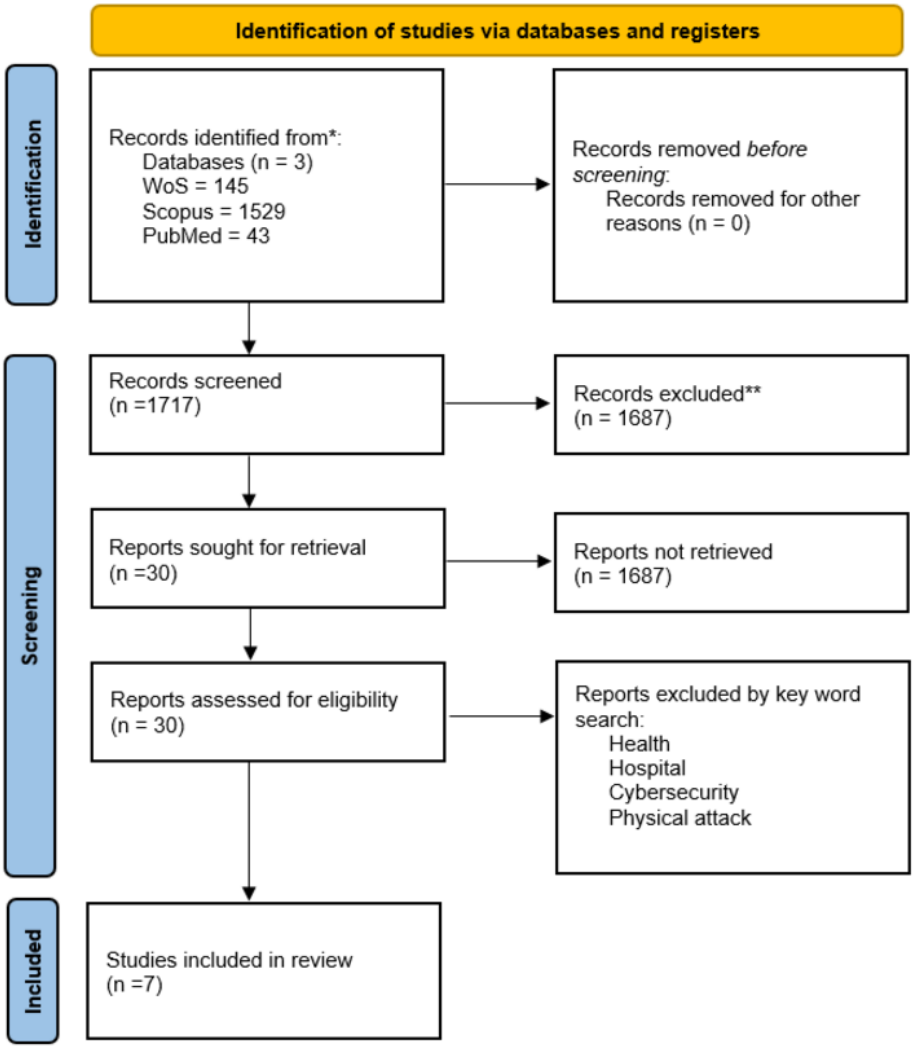

Figure 2. PRISMA flowchart. * The number of records identified from each database. ** Records excluded from the database based on search criteria.

2.4. Data Collection and Visualization

We then collected data from the relevant publications to conduct our analysis. We gathered basic information about the publications: title, authors, publication type, publication domain, and publication year. The basic information we collected led us to focus on two fields of interest—side-channel attacks and healthcare. Figure 3 visualizes the spectrum attack search between 2003 and 2022 through the Power BI Microsoft platform [14] and shows that computer science and medical informatics had the most spectrum attack publications, followed by the engineering and telecommunication domain.

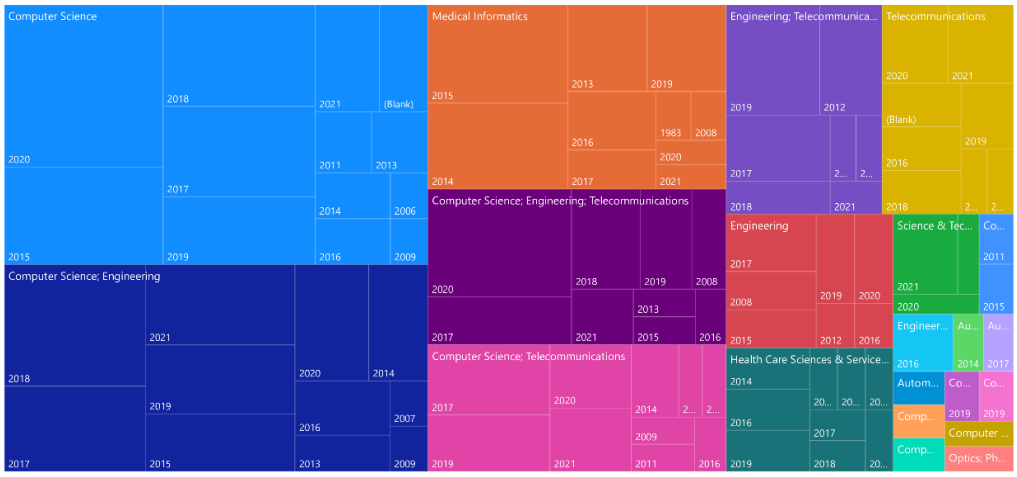

Figure 3. Physical layer attack search from PubMed and WoS categorized by research field.

Figure 4 shows spectrum attack publications in the institute of electrical and electronics engineers (IEEE) access, sensors, wireless personal computing, journal of medical internet research (JMIR), and association of computer machinery (ACM) computing, followed by other journals between 2003 and 2022. However, few studies on sniffing and replay attacks in health care show a significant research gap (Table 2) in IoMT RF attacks.

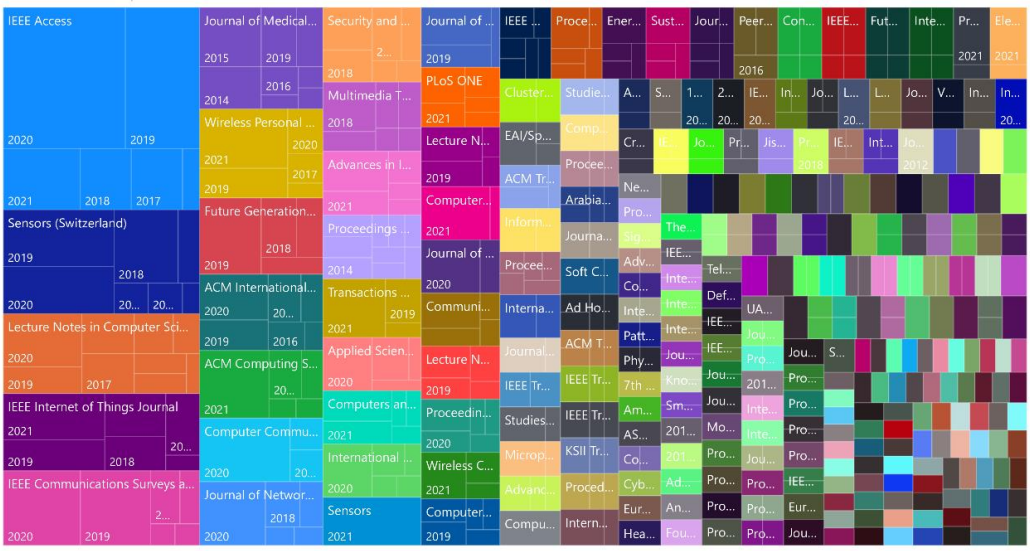

Figure 4. Physical layer attack search from Scopus categorized by research field.

A full counting relevance study is shown in Figure 5. The content is visualized based on the number of occurrences of a term exceeding 10 (143 terms from 5219). The Each term is given a relevance score. Based on this score, the most relevant term is selected. The default choice is 60% of the most relevant term. The small size of the red bubble with replay attack and the light blue bubble with side-channel attack indicate significant research gaps in those areas [17].

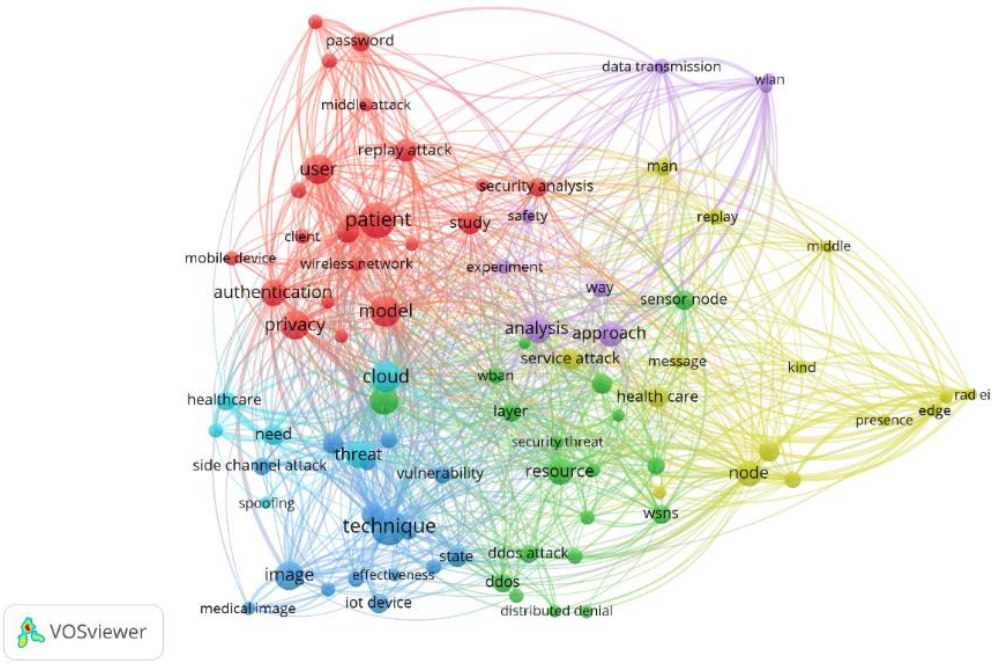

Figure 5. Relevance and occurrence study-full counting.

Figure 6 shows the binary counting relevance study. A VOS viewer [18] shows a visualization of the content based on the number of occurrences of a term greater than 10 (104 from 5219 terms). Each term is given a relevance score. Based on this score, the most relevant term is selected. The default choice is 60% of the most relevant term. Regarding the replay attack, the relevant keyword topics are well connected with other key terms highly prone to spectrum attacks [18]. The red bubble illustrates a method or attributes research gap in relation to replay attack, and the light blue and green bubbles indicate significant research gaps in the side-channel attack.

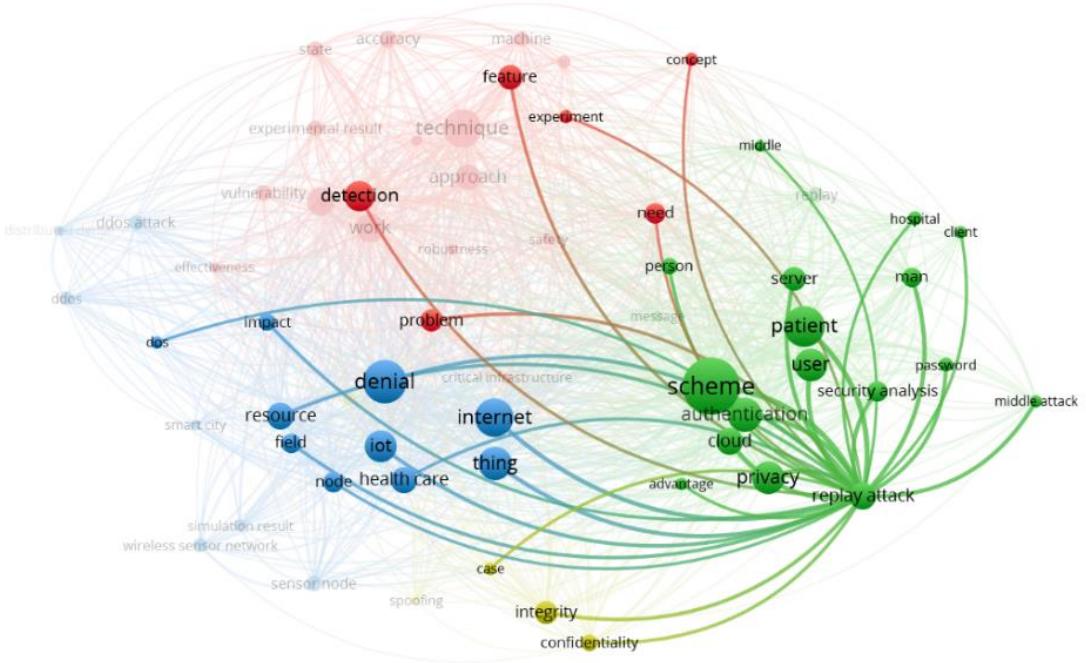

Figure 6. Relevance and occurrence study—binary counting.

2.5. Search Strategy and Selection Criteria

During the selection process, duplicate articles were removed, article titles were reviewed, and articles that did not pertain to IoT cybersecurity in healthcare were removed. We selected these articles based on information in our indexed database. Table 4 shows the attacks identified in WoS, Scopus, and PubMed. In Table 5, we list the attacks that are excluded. The articles that conceptualized specific use cases were retained, while those containing editorials, letters, reviews, and opinions not listed in Section 2.3 were excluded.

Table 4. The included articles.

Attacks	Web of Science	Scopus	PubMed
Jamming Attack	17	330	0
Replay Attack	50	372	23
Side-Channel Attack	30	447	0
Sniffing Attack	0	18	1
Spoofing Attack	23	316	5
Tampering Attack	25	46	14
Total	145	1529	43

Table 5. The excluded articles.

Attacks	Web of Science	Scopus	PubMed
Jamming Attack	16	330	0
Replay Attack	49	371	22
Side-Channel Attack	29	446	0
Sniffing Attack	0	18	1
Spoofing Attack	23	316	5
Tampering Attack	24	46	14
Total	141	1527	42

2.6. Data Generalization

We developed a standardized form using Microsoft Excel to evaluate the selected articles. The findings of heterogeneous studies were synthesized using a narrative review approach to describe IoT signal attack protocols, platforms, or functional prototypes. In the narrative review, individual and meta-analysis biases were not assessed, so missing data were eliminated.

3. Results and Discussion

The purpose of this section is to discuss the results retrieved from the publications and discuss two research questions.

1. RQ1: How well has IoT been integrated into health care?

We completed a systematic analysis of research articles per year against research for jamming [19], replay [20], sniffing [21], spoofing [20,22], side-channel, and tampering attacks in the web of science PubMed and Scopus. The results clearly show that computer and wireless communication domains are dominant, and the research articles are distributed in sensing layer attacks of IoMT. Table 1 and Figure 4 show the search analysis of cyber spectrum attacks across journals as per the PRISMA checklist in Appendix A. The Scopus papers containing terms about "jamming attack" and "health" yielded 330 rows, and the investigation on WoS yielded 17 articles. Scopus papers containing terms about "replay attack" and "health" yielded 372 rows, PubMed yielded 23 rows, and WoS yielded 50 articles.

Scopus papers containing terms about "side-channel attack" and "health" yielded 447 rows, and articles on WoS yielded 30 articles. Scopus papers containing terms about "sniffing attack" and "health" yielded 18 rows, PubMed yielded 1 row, and WoS yielded

0 articles. Scopus for papers containing terms about "spoofing attack" and "health" yielded 316 rows, PubMed yielded five, and WoS yielded 23 articles. Scopus papers containing terms about "tampering attack" and "health" yielded 25 rows, and articles on PubMed yielded 14 rows, and articles on WoS delivered 46 articles. This row-level analysis result reveals no significant research contribution in sniffing attacks on IoMT devices, and that trend follows with tampering attacks, etc.

Table 3 shows SLR from Sections 3.1–3.5 in tabular form. Section 3.1 reviews the cyber impacts and attacks on three-layer IoT architecture to identify the possibility of compromising adversaries' assets. Moreover, unethical hacking competencies and the corresponding core behaviors in weaponizing the SDR and radiofrequency to take over critical information such as client and clinical data repository from IoMT will significantly damage the entire healthcare user experience. We have well-established standard models and best practices with health level Seven international (HL7) [23] and fast health care interoperability resource (FHIR) [24] to meet health insurance portability accountability Act (HIPAA) compliance [25]. However, few studies on radio attack analysis on IoMT data and radio frequency machine learning framework have good wireless physical security risk mitigation strategies.

Section 3.2 studies attacks on physical layer protocol on the internet of things. The above review provides a roadmap for understanding RF physical attacks, including jamming, sniffing, spoofing, tampering, and replay attacks. In the upcoming Sections 3.3 and 3.4, we discuss the paper related to the testbed implementation for IoT field experimentation.

2. RQ2: What is the current state of healthcare-RF cybersecurity research?

3.1. Cyber Impacts and Layered Attacks

Criminality is uprooted from cybercrime, regardless of the attacking layer. By understanding cyber impacts at the human and OSI layers, we gained insight into the causes and were able to deploy countermeasure strategies against powerful attacks. Prior to reviewing the physical layer attacks, we will examine layered attacks and cybersecurity frameworks.

The research [26] examines threats, vulnerabilities, and attacks. Literature reviews, surveys, articles, repositories, attacks, incidents, and more demonstrated how cybersecurity harnesses multiple dimensions of the corporate ecosystem. Cyber harness themes were examined from adversaries' perspectives. According to the research, the taxonomy will enable companies to distinguish between high-value and low-value assets and how they are directly and indirectly associated with cyber-related harms. To improve their cybersecurity management program, the paper analyzed the VERIS community database (VCDB) [27].

3.1.1. Cyber-Attacks Taxonomy

In cyber-harm, five themes are distinguished: physical damage, theft, destruction, infection, exposure, corruption, performance reduction, pain, death, prosecution, and mistreatment.

Economic harm (disruptions of operations, sales, customers, growth, profits, extortion, joblessness, and scams).

Anger, shame, guilt, guilt, worthlessness, reduced satisfaction, and incorrect perceptions are all physical cyber-harms.

A reputational cyber-harm (leading to damage to public perception, brand damage, customer-corporate damage, and decreased business opportunities).

As a result of social cyber-harm, dynamic inconsistencies in public opinion are caused, cultural efficacy is disrupted, a negative impact is incurred on communities, and perceptions of organizational behavior are reduced.

The author proposes to extend their future work on an asset-oriented model for the corporate ecosystem and identifying high-value and low-value assets, and how the critical stakeholders involved in the interest of direct and indirect harm. However, this approach does not provide analytics or tools for advanced prediction or intelligent cybersecurity systems to help corporations understand cyber-harm. Despite not focusing on a specific

theme, their approach was sufficiently flexible and highly scalable. The data were sourced from an open-source database. The Vocabulary for Event Recording and Incident Distribution System (VERIS) framework is loaded with open-source cybersecurity key performance indicators (OCKPI) to identify the security incident insights, increase the companies' risk mitigation strategies, and extend that framework for effective incident handling mechanism [28]. This framework provides details related to incident insights. It classifies incidents based on external, internal, and partner-based threats. It also provides insights into hacking evidence, including IoT forensics, malware behavior, social engineering attacks, privilege misuse, known and unintentional errors, and how confidentiality, integrity, and availability are affected through critical metrics.

The key metrics on incidents are classified based on victims (size of the organization), actors, actions, assets, attributes, timelines, impacts, and repeated events. Moreover, this framework provides facilities to understand the efficacy of a business continuity plan through the discovery and response process targeting how the discovery is processed, the root causes, and the corrective actions. How do you differentiate between targeted and opportunistic attack scenarios? This data-driven framework gives greater visibility and reasoning on the key performance indicators. However, the open-source community lacks the credibility of data and future support.

3.1.2. Cyber Security Framework

A security framework assessment matrix compares various cybersecurity framework implementation trends [29]. Authors performed through literature review and qualitative document analysis. The cybersecurity framework's assessment matrix helps identify how many items are covered. Besides, three frameworks from three countries are aligned to their country profile and risk management strategies. According to the investigation, their analysis benefits policymakers and executives doing business in three states by improving their framework strength and understanding of necessary improvements. In addition, country-specific cybersecurity implementation frameworks (CIFs) were implemented across regions, and business values were shared. Hence, evidence-based insights are developed for decision-makers from business regions to improve their existing cybersecurity frameworks. However, most action items are derived from the NIST framework except for risk governance, which had substantial quantitative empirical support. NIST's limitations are prioritized in this paper, but most action items are still inherited from NIST.

Moreover, the author used the old policy-2014 instead of the amended policy-2018 for the Australia protective security policy framework (PSPF) assessment. To improve cybersecurity framework implementation, the authors analyzed the assessment matrix and used pattern-matching [30]. On the other hand, there is a potential gap in enhancement to understand the effectiveness of adopting and utilizing cybersecurity implementation frameworks, though adopted by businesses having branch offices across those regions (the UK, Australia, and the USA).

3.1.3. Cyber-Attacks Classification

Based on the open systems interconnection (OSI) model, the author [31] develops strategies to defend against attacks across industries. The research explains the three-layer architecture: The top layer, the application layer, comprises intelligent processing, cloud computing, middleware technologies, and service platforms. Wireless local area networks (WLAN), GPS, and internet protocol (IP) make up the network layer. Lastly, the sensing layer includes all IoT technologies, including RFID, NFC, Wi-Fi, computer vision, and coordination. Despite the growing demand for contactless sensing, SOLI may lead to multilayer architectures. Furthermore, the research explains various attacks on the three-layer IoT architecture. The various attacks are physical attacks, jamming attacks [32], relay attacks [33], sybil, selective forwarding, side-channel attacks [20], replay, evil twin [34], sniffing [35], spoofing, tampering or malicious code injection, firmware attacks, and network layer attacks (sinkhole, unfairness, incorrect routing, session flooding,

eavesdropping related to packets). Application layer (phishing attacks virus, worms, spyware, malicious scripts, denial-of-service (DOS), injection, buffer overflows, RFID tampering. However, they demonstrated goal-based classification of the evolving signal security threats and spectrum-level vulnerabilities, causing significant disruption to the OSI. Those attacks are not limited to frequency hopping spread spectrum attack [36], direct sequence spread spectrum [37], or chirp spread spectrum (CSS) hybrid. The research investigates criminality or attacking goal-based layered classification and still lacks the choice of methodology, validation, and future works.

The research investigates criminality or attacking goal-based layered classification and still lacks the choice of methodology, validation, and future works.

3.2. Cyber-Physical Attacks on Protocols

This paper [38] examines the effectiveness of IoT against high-power cellular networks using various low-power protocols. The author discusses the key technical differences between Sigfox, LoRa, and NB-IoT, as well as their advantages and disadvantages. According to their investigation, specific protocols will deliver high mobility and QoS. However, downlink data are possible with wearables with the same spectrum threat of the uplink process.

In other words, the danger is not different for each process since both work under an unlicensed frequency band under the range of Industrial, scientific, and medical (ISM) 900 MHZ [39]. Medical sensors in the ISM band are vulnerable to physical layer attacks. Examples include tampering/malicious code injection, firmware attacks, jamming, replay, and evil twin attacks. During the reconnaissance phase of attack strategies, adversaries thoroughly investigate those devices. OSINT toolsets are suited to their motivations and guided by attack vector maturity. The newly identified markers employ a variety of attack surfaces, including iron oxide fillings and traces. In our scope, we focus on attacks at the spectrum level before reaching the IP network gateway. A few common attacks on those spaces are sniffing, eavesdropping, jamming, network state disruption or transmitting noise, and conflicting the traffic within the target RF channel having the same frequency.

Re-transmitting the symbol or captured frames to the receiver to implement a replay attack includes re-transmitting mutated information. The threat or aggression process will be the same regardless of the spectrum of attacks. The base of any attack strategy is to understand the protocols and reverse engineer the spectrum for payload injection. Several factors contribute to the identification and localization, including modulation, frequency, bandwidth, data rate, half duplex or full duplex system, maximum payload size, range between source-target, interference immunity, adaptive data rate, authentication, handover to fault-tolerant node, localization, and energy awareness. Additionally, the localization of the transmitting rogue SDR is detectable using the angle of arrival (AOA), time difference of arrival (TDOA), frequency difference of arrival (FDOA), and received signal strength indicator (RSSI) techniques.

Cyber-Physical Attacks on Low-Power Protocols

In paper [39], the author examines the effectiveness of the Internet of Things using low-power protocols. Furthermore, their investigation claims that mobility and QoS will be high for specific protocols because of asset mobility and continuous evaluation and monitoring. The IoT, drones, radio channels, satellite communications, and marine, aeronautical, and deep space communication create new cybersecurity threats. Anything emitting RF energy is vulnerable. Due to IoT, including the internet of medical things, battle things, and the internet of everything, and high-level adversary motivation, the attack surface is growing. New threats will increase the urgency for innovation in frameworks, cybersecurity maturity models, standards, and guidelines. Therefore, cybersecurity policies and controls must move into the extended maturity group.

3.3. Sniffing Attack

This section discusses physical attacks—sniffing and tampering. However, little is known about how the Internet of Medical Things matures and how Radio Frequency spectrum attacks have grown in recent years. There is a niche gap in the research's demonstration evaluation depth and rigor [40] on side-channel attacks on wearables. The categorization of attack levels—operating system level, user interface level, shows how the sensitive information across the process flows. However, there are no concrete details on contribution. Finally, the inheritance of old password authentication strategies shows the infancy of research rigor and does not contribute to sniffing attacks. An analysis compared solutions against IoT attacks, dividing them into three layers, focusing on perception layer attacks and further dividing perception layer attacks by technology. The contribution of this paper [41] goes beyond the practice of designing, making artifacts, proving concepts, doing experiments, evaluating them, and making suggestions for the future. Motivating research focus with possible questions is the main idea.

3.4. Cybersecurity Experimentation with AI-Enabled CS

The paper [42] explores artificial intelligence (AI) cybersecurity systems. A platform is needed to test big data and fog computing, cyber situational awareness, innovative simulations, and cyber decision support systems (CDSS). For example, safety-critical systems include production and industrial control systems (ICS), and mission-critical includes communication, access management, interfaces, and business system (HRM, financial, procurement, product, innovation, sales, marketing, etc.). The corporate system cannot depend only on the external penetration testing strategies but develop an internal red team—to attack the system—and a blue team—to defend the system—providing a competitive advantage in attaining cyber maturity. To achieve and reduce the dependability on external penetration tester, the low-cost testbed can be performed to improve the effectiveness and usability of continuous security monitoring (CSM), facilitate attack and defense awareness among employees, and thus reduce KT cost between IT and operational departments. The testbed can also be scaled to accommodate upcoming threats from similar market segments and innovate new strategies—deception against advanced persistent threats (APTs).

Researchers state that the inability to experiment with cybersecurity threats on the low-cost testbed is an excellent threat to the ICS. The research claims that open-source hardware and software can develop a testbed within 500 euros for ethical industrial control system hacking, education, competency development, and research. However, it lacks rationality in the choice of hardware and software concerning functional and non-functional attributes such as performance, security, scalability, maintainability, interoperability, usability, and availability. Additionally, this approach will improve the real-world simulation of attack and defense strategies discussed in the previous paper. This approach motivates us to identify a cost-effective way to conduct field experiments as we implement our framework. Using interoperable data-driven systems, the research examines the industry 4.0 problem.

Additionally, they investigated the four levels of cybersecurity in ICS and how intruder threats, including insider threats, can experiment against them. Based on the analysis, insider threats and associated tools impact 0 and 1 compared to a remote intruder. The author demonstrated that a low-cost testbed could address the growing demand for attack vectors and surfaces in the corporate ecosystem. Expert assessments and other studies are recommended for fog computing and AI-enabled systems [43].

Using low-cost SDR hardware and universal radio hacker (URH), we have developed a framework and validated attack and defense scenarios in the hospital ecosystem [42].

3.5. Radiofrequency Machine Learning and Data Set Creation

ML and DL techniques are analyzed in a paper [44] on network-centric intrusion detection systems (IDS). This paper provides an overview of publicly available cyberse-

curity intrusion detection data sets. Due to inconsistent support categories, there may be insufficient data volume to address research objectives.

In this paper [45], the author examines endpoint detection and response (EDR). They then demonstrated how data-driven technologies are replacing traditional approaches. Between 1990 and 2019, they studied IEEE, Science Direct, ACM, and Springer Link databases. Alternative methodologies are available for endpoint detection and response (EDR). The research aims to analyze the publication trends in EDR and techniques used for EDR. However, they do not address how ML and DL can be used for intelligent systems. Each of the four categories of machine learning algorithms is represented in cybersecurity management systems (supervised learning, unsupervised learning, semi-supervised learning, reinforcement learning). Using design science principles, each category represents a unique set of machine learning algorithms. EDR technologies such as fire eye endpoint security [46], carbon black response [47], Symantec endpoint protection, Webroot endpoint protection, etc., can be improved through optimized data-driven cybersecurity processes.

Future research will need to examine how these ML techniques are used with analytics and tools for advanced prediction or intelligent sniffing systems. No evidence or reason was provided for their choice of four databases. The cybersecurity core systems (governance, risk management, information security control, compliance, audit, security program management, operation, information security core module, strategic planning, finance, procurement, innovation, and vendor ecosystem) are a top hierarchy. Additionally, their associated subsystems (compliance management, guidelines, program management, operation management, access control, physical security, network security, endpoint protection, application security, encryption technologies, virtualization, cloud computing, transformative technologies, strategic planning, designing, developing, and maintaining information security program, awareness, education) are categorized as middle-level categories.

Dimensions and facts include security metrics and measurable quantities. The dimensions against those facts are viewed by region, time, incidents, threats, vulnerabilities, assets, and attacks. Frameworks are developed with multilayer architectures (database, business, presentation, and innovation). Cardinalities from the azure cloud synapse and data brick [48] connect dimensions and facts in the database layer. The business layer implements business logic and security logic, including embedded and available filters. The presentation layer, query items (columns), and query subjects (table) are reflected as functional requirements, non-functional requirements, policies, and data governance. Dimensions such as time, date, and asset are critical, as well as malware infection facts, threats, vulnerabilities, configurations, mitigations, protocol, transmission power, and reception power.

Our research identifies gaps, develops frameworks and prototypes, and validates them through experiments and analysis. RFML provides insight into how deep learning technologies could be used for identifying modulation and spectrum information and their signal classification.

4. Conclusions and Future Works

The PRISMA-based search and systematic literature review identify the research gap in radio frequency spectrum threats in the hospital ecosystem. The potential gap is well analyzed, and the results are visualized. This research paper will be relevant to the IoT, IoMT, and medical readers, as this will open a new dimension for physicians and healthcare researchers in spectrum-level threats in machine implantable communication systems. Examples: deep brain stimulators, implantable cardioverter-defibrillator, cardiac stents, implantable insulin pumps, interocular lenses, and pacemakers.

Time difference of arrival (TDOA)-based IoMT field experimentation will be used in our future research to validate the defensive framework. The framework will guide healthcare stakeholders while implementing corporate cybersecurity strategies.

Eventually, further analysis will answer why and how sniffing attacks occur and how they can be identified and mitigated. We will use the design science research methodology

to validate the entire process. A core research problem is identified as part of the first agile process, motivating the researcher and customer toward solutions. An overview of the issue and the importance of finding solutions are provided. As part of the second agile process, solutions are evaluated qualitatively, quantitatively, or using a combination of methods. An artifact's core behavior and structure are deduced by analyzing the created solutions during the third agile process. The fourth, the agile methodology, shows how well you can create artifacts that solve problems through design and development. We planned to perform extensive experiments, simulations, and proofs-of-concept to understand how the artifacts address the core issues. As part of the fifth agile process, the success criteria are compared with the findings or results.

We are measuring and observing how artifacts support solutions to problems. The proposed solutions' objectives are well matched with the experimental findings through demonstration processes. As a result of this process, researchers can improve artifacts and communicate results for further development. At the end of the agile process, findings will be communicated in relation to the published objectives for peer review. Our proposed future research investigates sniffing attacks on IoMT under the medical implantable communication system (MICS) frequency band ranging from 402 to 406 MHZ using the design science method.

We planned to use radio frequency machine learning (RFML) utilizing radio frequency machine learning [49], physical emanation security [50], and the internet of medical things. We will develop an open-source testbed for collecting signal intelligence data. We develop a proposed framework for countering or mitigating RF spectrum-based sniffing attacks on IoMT in the healthcare ecosystem. The results and analysis will be evaluated in the testbed. Research issues in spectrum-level physical attacks on IoMT devices will be discussed, including future directions and commercialization.

Author Contributions: Conceptualization, I.A.J. and B.S.; methodology, I.A.J. and B.S.; software, B.S. and S.A.; validation, B.S., S.A. and G.N.S.; formal analysis, I.A.J.; investigation, B.S. and S.A.; resources, S.A.; data curation, I.A.J.; writing—original draft preparation, I.A.J. and B.S.; writing—review and editing, I.A.J.; visualization, I.A.J. and B.S.; supervision, B.S. and S.A.; project administration, S.A. and G.N.S. All authors have read and agreed to the published version of the manuscript.

Funding: The research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: https://github.com/VaccineResearch/RF_SLR.

Acknowledgments: The authors would acknowledge the support of the Internet of Things Lab and Energy Resources Institute, Charles Darwin University.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. SLR Protocol.

The Objective
A Systematic Review of Radio Frequency Threats in IoMT.
Research Questions
RQ1: How well has IoT been integrated into healthcare? RQ2: What is the current state of healthcare-RF cybersecurity research?

Table A1. *Cont.*

The Objective
A Systematic Review of Radio Frequency Threats in IoMT.
Research Questions
RQ1: How well has IoT been integrated into healthcare? RQ2: What is the current state of healthcare-RF cybersecurity research?
Literature Reviewers
Primary reviewer: Mr. Irrai Anbu Jayaraj, Energy and Resources Institute, College of Engineering, IT and Environment, Charles Darwin University, NT, Australia. Second reviewer: Dr. Bharanidharan Shanmugam, Energy and Resources Institute, College of Engineering, IT and Environment, Charles Darwin University, NT, Australia. Third reviewer: Dr. Sami Azam, College of Engineering, IT and Environment, Charles Darwin University, NT, Australia.
Methodology of search
Search Terms:ALL (“JAMMING ATTACK”) AND ALL (“HEALTH”) AND PUBYEAR > 2002 ALL (“REPLAY ATTACK”) AND ALL (“HEALTH”) AND PUBYEAR > 2002 ALL (“SNIFFING ATTACK”) AND ALL (“HEALTH”) AND PUBYEAR > 2002 ALL (“TAMPERING ATTACK”) AND ALL (“HEALTH”) ALL (“SIDE CHANNEL ATTACK”) AND ALL VAND PUBYEAR > 2002 ALL (“DENIAL ATTACK”) AND ALL (“HEALTH”) AND PUBYEAR > 2002 ALL (“SPOOFING”) AND ALL (“HEALTH”) AND PUBYEAR > 2002
The following databases are included:
Web of Science (WoS), Scopus, and PubMed
Process of evaluation (POE)
POE1: Range: Evaluations are based on the date range (2003–2022) and originality of the studies. POE2: Relevance: During the screening process, titles and abstracts are checked for relevance to IoMT in attacks on physical layers. POE3: Inclusion: Studies are evaluated against inclusion criteria. The inclusion of any study that does not meet all the criteria is discarded. POE4: Specificity: Checking whether the studies relate closely enough to the defined research field of IoMT in healthcare cybersecurity. POE5: Data: Data related to the research questions and contributions are analyzed for selected studies.
Criteria for the study
Inclusion Criteria (I)I1: The original research study was conducted by the corresponding author. I2: A publication about IoT and cybersecurity at the physical layer. I3: Research findings should be adequately explained in publications. I4: Years of publication between 2003 and 2022. Exclusion Criteria (E) E1: Reviews of the literature, secondary research, and other publications that are not related to the topic. E2: Publications that contain only ideas, such as magazines, interviews, and discussion papers. E3: Non-English publications.
Report
A spreadsheet is used to record and analyze findings.

References

1. Guri, M. MAGNETO: Covert channel between air-gapped systems and nearby smartphones via CPU-generated magnetic fields. *Future Gener. Comput. Syst.* **2021**, *115*, 115–125. [CrossRef]
2. Guri, M.; Zadov, B.; Elovici, Y. ODINI: Escaping Sensitive Data From Faraday-Caged, Air-Gapped Computers via Magnetic Fields. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 1190–1203. [CrossRef]
3. Mirsky, Y.; Guri, M.; Elovici, Y. HVACKer: Bridging the Air-Gap by Attacking the Air Conditioning System. *arXiv* **2017**, arXiv:1703.10454.
4. Guri, M.; Bykhovsky, D. aIR-Jumper: Covert air-gap exfiltration/infiltration via security cameras & infrared (IR). *Comput. Secur.* **2019**, *82*, 15–29.
5. Kang, S.-G.; Song, M.-S.; Kim, J.-W.; Lee, J.W.; Kim, J. Near-Field Communication in Biomedical Applications. *Sensors* **2021**, *21*, 703. [CrossRef]

6. Gomez, C.; Oller, J.; Paradells, J. Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology. *Sensors* **2012**, *12*, 11734–11753. [CrossRef]
7. Pahlavan, K.; Krishnamurthy, P. Evolution and Impact of Wi-Fi Technology and Applications: A Historical Perspective. *Int. J. Wirel. Inf. Netw.* **2021**, *28*, 3–19. [CrossRef]
8. Koutras, D.; Stergiopoulos, G.; Dasaklis, T.; Kotzanikolaou, P.; Glynos, D.; Douligeris, C. Security in IoMT Communications: A Survey. *Sensors* **2020**, *20*, 4828. [CrossRef]
9. Aygun, I.; Kaya, B.; Kaya, M. Aspect Based Twitter Sentiment Analysis on Vaccination and Vaccine Types in COVID-19 Pandemic With Deep Learning. *IEEE J. Biomed. Heal. Inform.* **2022**, *26*, 2360–2369. [CrossRef]
10. Pati, D.; Lorusso, L.N. How to Write a Systematic Review of the Literature. *HERD* **2018**, *11*, 15–30. [CrossRef]
11. Kuckertz, A.; Block, J. Reviewing systematic literature reviews: Ten key questions and criteria for reviewers. *Manag. Rev. Q.* **2021**, *71*, 519–524. [CrossRef]
12. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. Available online: https://www.mdpi.com/2079-9292/11/2/198/htm (accessed on 23 February 2022).
13. Kelly, J.T.; Campbell, K.L.; Gong, E.; Scuffham, P. The Internet of Things: Impact and Implications for Health Care Delivery. *J. Med. Internet Res.* **2020**, *22*, e20135. [CrossRef] [PubMed]
14. Edwards, T. Reviews: British Standards Institution: Glossary of documentation terms. BSI, I976. 8Ipp. BS 5408: I976. £8.20. ISBN o 580 09407 3. *J. Librariansh.* **1977**, *9*, 235–239. [CrossRef]
15. Blažič, B.J. Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? *Educ. Inf. Technol.* **2021**, *27*, 3011–3036. [CrossRef]
16. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Syst. Rev.* **2021**, *10*, 89. [CrossRef]
17. Perianes-Rodriguez, A.; Waltman, L.; van Eck, N.J. Constructing bibliometric networks: A comparison between full and fractional counting. *J. Inf.* **2016**, *10*, 1178–1195. [CrossRef]
18. van Eck, N.J.; Waltman, L. Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics* **2010**, *84*, 523. [CrossRef]
19. Ferreira, R.; Gaspar, J.; Sebastião, P.; Souto, N. Effective GPS Jamming Techniques for UAVs Using Low-Cost SDR Platforms. *Wirel. Pers. Commun.* **2020**, *115*, 2705–2727. [CrossRef]
20. Greene, K.; Rodgers, D.; Dykhuizen, H.; McNeil, K.; Niyaz, Q.; Shamaileh, K.A. Timestamp-based Defense Mechanism against Replay Attack in Remote Keyless Entry Systems. In Proceedings of the 2020 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 4–6 January 2020; pp. 1–4.
21. Huang, S.; Lin, C.; Zhou, K.; Yao, Y.; Lu, H.; Zhu, F. Identifying physical-layer attacks for IoT security: An automatic modulation classification approach using multi-module fusion neural network. *Phys. Commun.* **2020**, *43*, 101180. [CrossRef]
22. Shafiee, E.; Mosavi, M.R.; Moazedi, M. Detection of Spoofing Attack using Machine Learning based on Multi-Layer Neural Network in Single-Frequency GPS Receivers. *J. Navig.* **2017**, *71*, 169–188. [CrossRef]
23. Bender, D.; Sartipi, K. HL7 FHIR: An Agile and RESTful approach to healthcare information exchange. In Proceedings of the 26th IEEE International Symposium on Computer-Based Medical Systems, Porto, Portugal, 20–22 June 2013; pp. 326–331.
24. Hong, N.; Wang, K.; Yao, L.; Jiang, G. Visual FHIR: An Interactive Browser to Navigate HL7 FHIR Specification. In Proceedings of the 2017 IEEE International Conference on Healthcare Informatics (ICHI), Park City, UT, USA, 23–26 August 2017; pp. 26–30.
25. Nahra, K.J. HIPAA Security Enforcement Is Here. *IEEE Secur. Priv.* **2008**, *6*, 70–72. [CrossRef]
26. Agrafiotis, I.; Nurse, J.; Goldsmith, M.; Creese, S.; Upton, D. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *J. Cybersecur.* **2018**, *4*, tyy006. Available online: https://academic.oup.com/cybersecurity/article/4/1/tyy006/5133288 (accessed on 24 August 2020). [CrossRef]
27. Cremer, F.; Sheehan, B.; Fortmann, M.; Kia, A.N.; Mullins, M.; Murphy, F.; Materne, S. Cyber risk and cybersecurity: A systematic review of data availability. *Geneva Pap. Risk Insur.-Issues Pract.* **2022**, *47*, 698–736. [CrossRef]
28. Moreira, G.B.; Calegario, V.M.; Duarte, J.C.; dos Santos, A.F.P. Extending the VERIS Framework to an Incident Handling Ontology. In Proceedings of the 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), Santiago, Chile, 3–6 December 2018; pp. 440–445.
29. Dedeke, A.; Masterson, K. Contrasting cybersecurity implementation frameworks (CIF) from three countries. *Inf. Comput. Secur.* **2019**, *27*, 373–392. [CrossRef]
30. Lejins, Y.; Leitch, J. A Holistic Approach to eHealth Security in Australia: Developing a National eHealth Sercurity and Access Framework (NESAF). Australian eHealth Informatics and Security Conference. 2012. Available online: https://ro.ecu.edu.au/aeis/8 (accessed on 24 February 2022).
31. Mouaatamid, O.E.; Lahmer, M.; Belkasmi, M. Internet of Things Security: Layered classification of attacks and possible Countermeasures. *Electron. J. Inf. Technol.* **2016**, 66–80. Available online: http://www.webmail.revue-eti.net/index.php/eti/article/view/98 (accessed on 28 September 2020).
32. Hamza, T.; Kaddoum, G.; Meddeb, A.; Matar, G. A Survey on Intelligent MAC Layer Jamming Attacks and Countermeasures in WSNs. In Proceedings of the 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), Montreal, QC, Canada, 18–21 September 2016; pp. 1–5.

33. Patil, M.M.; Hanni, A.; Tejeshwar, C.H.; Patil, P. A qualitative analysis of the performance of MongoDB vs. MySQL database based on insertion and retriewal operations using a web/android application to explore load balancing—Sharding in MongoDB and its advantages. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017; pp. 325–330.
34. Agarwal, M.; Biswas, S.; Nandi, S. An Efficient Scheme to Detect Evil Twin Rogue Access Point Attack in 802.11 Wi-Fi Networks. *Int. J. Wireless Inf. Netw.* **2018**, *25*, 130–145. [CrossRef]
35. Lichtman, M.; Jover, R.P.; Labib, M.; Rao, R.; Marojevic, V.; Reed, J.H. LTE/LTE-A jamming, spoofing, and sniffing: Threat assessment and mitigation. *IEEE Commun. Mag.* **2016**, *54*, 54–61. [CrossRef]
36. Giustiniano, D.; Schalch, M.; Liechti, M.; Lenders, V. Interference Suppression in Bandwidth Hopping Spread Spectrum Communications. In *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec '18), Stockholm, Sweden, 18–20 June 2018*; Association for Computing Machinery: New York, NY, USA, 2018; pp. 134–143. [CrossRef]
37. Wullems, C.; Tham, K.; Smith, J.; Looi, M. A trivial denial of service attack on IEEE 802.11 direct sequence spread spectrum wireless LANs. In Proceedings of the 2004 Symposium on Wireless Telecommunications, Pomona, CA, USA, 14–15 May 2004; pp. 129–136.
38. Mekki, K.; Bajic, E.; Chaxel, F.; Meyer, F. A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express* **2019**, *5*, 1–7. [CrossRef]
39. Kumbhar, A. Overview of ISM Bands and Software-Defined Radio Experimentation. *Wirel. Pers. Commun.* **2017**, *97*, 3743–3756. [CrossRef]
40. Nahapetian, A. Side-channel attacks on mobile and wearable systems. In Proceedings of the 2016 13th IEEE Annual Consumer Communications Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2016; pp. 243–247.
41. Khattak, H.A.; Shah, M.A.; Khan, S.; Ali, I.; Imran, M. Perception layer security in Internet of Things. *Future Gener. Comput. Syst.* **2019**, *100*, 144–164. [CrossRef]
42. Sauer, F.; Niedermaier, M.; Kießling, S.; Merli, D. LICSTER—A Low-cost ICS Security Testbed for Education and Research. *arXiv* **2019**, arXiv:191000303.
43. Abdulkareem, K.H.; Mohammed, M.A.; Gunasekaran, S.S.; Al-Mhiqani, M.N.; Mutlag, A.A.; Mostafa, S.A.; Ali, N.S.; Ibrahim, D.A. A Review of Fog Computing and Machine Learning: Concepts, Applications, Challenges, and Open Issues. *IEEE Access* **2019**, *7*, 153123–153140. [CrossRef]
44. Xin, Y.; Kong, L.; Liu, Z.; Chen, Y.; Li, Y.; Zhu, H.; Gao, M.; Hou, H.; Wang, C. Machine Learning and Deep Learning Methods for Cybersecurity. *IEEE Access* **2018**, *6*, 35365–35381. [CrossRef]
45. Sjarif, N.N.A.; Chuprat, S.; Mahrin, M.N.; Ahmad, N.A.; Ariffin, A.; Senan, F.M.; Zamani, N.A.; Saupi, A. Endpoint Detection and Response: Why Use Machine Learning? In Proceedings of the 2019 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 16–18 October 2019; pp. 283–288.
46. Dujmić, M.; Delija, D.; Sirovatka, G.; Žagar, M. Using FireEye Endpoint Security for educational purposes. In Proceedings of the 2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, 28 September–2 October 2020; pp. 1206–1211.
47. Tselios, C.; Tsolis, G.; Athanatos, M. A Comprehensive Technical Survey of Contemporary Cybersecurity Products and Solutions. In *Computer Security*; Springer-Verlag: Berlin/Heidelberg, Germany, 2020; pp. 3–18.
48. Copeland, M.; Jacobs, M. Reduce Cyber Security Vulnerabilities: IaaS and Data. In *Cyber Security on Azure: An IT Professional's Guide to Microsoft Azure Security*; Copeland, M., Jacobs, M., Eds.; Apress: Berkeley, CA, USA, 2021; pp. 83–108.
49. Wong, L.J.; Clark, I.V.W.H.; Flowers, B.; Buehrer, R.M.; Michaels, A.J.; Headley, W.C. The RFML Ecosystem: A Look at the Unique Challenges of Applying Deep Learning to Radio Frequency Applications. *arXiv* **2020**, arXiv:201000432.
50. Khan, H.A.; Sehatbakhsh, N.; Nguyen, L.N.; Callan, R.L.; Yeredor, A.; Prvulovic, M.; Zajic, A. IDEA: Intrusion Detection through Electromagnetic-Signal Analysis for Critical Embedded and Cyber-Physical Systems. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 1150–1163. [CrossRef]