International Journal of Computational Intelligence in Control

Addressing Security Issues, Threats,Attacks and Challenges to Improve the Security Architecture of Internet of Medical Things

Mudasir Mahmood[1]*, Muhammad Ijaz Khan[1], Asia Zaman[1], Muhammad Farhan[1], Rameen Zahra Qureshi[1], Muhammad Salman[1], Waqas Ahmad[1]

mudasir@gu.edu.pk,
ijazkhan@gu.edu.pk
aasiazaman123@gmail.com
muhammadfarhan01@gmail.com
rameenzahra945@gmail.com
muhammadsalmankundi@gmail.com
waqaas171@gmail.com

1. Institute of Computing and Information Technology, Gomal University, Pakistan.

*Corresponding Author: mudasir@gu.edu.pk

Date of Submission:15th August 2021 Revised: 29th December 2021 Accepted: 14th January 2022

Abstract: -Ever since the emergence of the concept internet of things (IoT), it has been applied in many fields. In the area of medical sciences, a new concept "Internet of Medical Things" (IoMT) has erupted. It has covered a wide scope pertaining to health but unfortunately been facing many Security issues, threats,attacks and challenges in IoMT. Many studies have been conducted on this significant area but still, there a very few studiesare available which address the Security issues, threats,attacks and challenges in IoMT. In this study, we have conducted extensive and comprehensive Systematic LeteratureReview (SLR) and explored top ranking papers relating to the security of IoMT Stakeholders, Solutions and Archetectures along with their issues, threats,attacks and challenges. This study will be beneficial for future researchers who would be willing to improve existing security issues, threats,attacks and challenges in IoMT as well as for those who want to develop new security models for IoMT.

Keywords: Internet of Medical Things, Security, Issues, Threats,Attacks,Challenges, Healthcare, Privacy, IoT, Stakeholder.

1. Introduction:

The widespread adoption of Internet of Medical Things (IoMT) solutions in healthcare has revolutionized patient care and improved healthcare outcomes. IoMT solutions, such as wearable devices, sensors, and mobile apps, have enabled remote monitoring of patients, improved disease management, and provided real-time data to healthcare providers [1]. However, the widespread use of IoMT solutions also presents significant security risks, as sensitive patient data must be protected from potential threats and vulnerabilities, including cyberattacks, unauthorized access, and data breaches [2].

Traditional approaches to securing healthcare systems may not be sufficient to protect IoMT systems, which have unique security challenges due to the diversity of IoMT stakeholders, solutions, and architecture. IoMT stakeholders, including medical professionals, device manufacturers, and IT professionals, have different roles and responsibilities within IoMT systems, which can complicate the development and implementation of effective security measures [2,3]. IoMT solutions, such as medical devices and wearables, have limited computing power and may lack built-in security features. IoMT architecture, including network topology, data flow, and protocols, must also be considered when developing security measures for IoMT systems [4].

Currently, there is no comprehensive approach to securing IoMT systems that addresses these unique security challenges. Existing security frameworks may not fully account for the complex interactions among stakeholders, solutions, and architecture in IoMT systems [5]. As a result, there is an urgent need for a practical and effective IoMT Security Framework that can help ensure the confidentiality, integrity, and availability of patient data while also promoting the benefits of IoMT solutions.

The Internet of Medical Things (IoMT) is a network of medical devices, wearables, and sensors that are connected to the internet and can collect, store, and transmit data. IoMT solutions have revolutionized patient care and disease management by enabling remote monitoring, real-time data collection, and improved disease management. IoMT solutions can also reduce healthcare costs by reducing the need for in-person appointments and hospital visits [6,7].

IoMT solutions offer a multitude of benefits for patients and healthcare providers alike. Real-time data provided by IoMT solutions allow healthcare providers to monitor patients remotely and respond rapidly to medical emergencies [8]. IoMT solutions also empower patients by giving them greater control over their healthcare, enabling them to track their health data and communicate with healthcare providers more efficiently [9]. However, the widespread use of IoMT solutions also entails significant security risks. It is essential to protect sensitive patient data from potential threats and vulnerabilities, such as cyberattacks, unauthorized access, and data breaches. By addressing these security threats through a comprehensive and practical approach, such as the proposed IoMT Security Framework, the IoMT network can be safeguarded against potential threats and vulnerabilities, and sensitive patient data can be kept confidential and secure [10].

2. Research Problem:

The rapid growth and adoption of the Internet of Medical Things (IoMT) has revolutionized healthcare by providing real-time monitoring, remote diagnostics, and advanced patient care. However, the sensitive nature of medical data and the criticality of healthcare services have made IoMT a prime target for various security threats, attacks, and challenges [11-14]. Ensuring the privacy and integrity of patient data is paramount, and failure to address these security concerns can lead to significant consequences for both patients and healthcare providers. Despite the numerous studies on IoMT security, a comprehensive understanding of the current state of security architecture and the most effective methods to mitigate threats remains elusive. This study aims to conduct a systematic literature review (SLR) to investigate and synthesize the existing body of knowledge on IoMT security issues, threats, attacks, and challenges, with the goal of identifying potential improvements in the security architecture of IoMT systems.

3. Systematic Literature Review:

This SLR was conducted to identify and address security challenges and vulnerabilities in the IoMT ecosystem. The study aimed to conduct an SLR to identify security issues faced by different stakeholders, IoMT architecture, and solutions to enhance IoMT security.

Key approach used in this study are discussed as under:

3.1. Definition of Research Scope:

In this study, we recognize the need to find patterns and gaps relevant to the security issues, threats,attacks and challenges. As a result, it is required to choose a few research questions (RQ) from the primary studies' inputs, which came from the analysis of pertinent studies.

Research Questions:

Primary Question

RQ1: How to improve the Security Architecture of IoMT?

Secondary Question

RQ2: What are the specific security issues, threats,attacksand challenges facing IoMT stakeholders?

RQ2.1: What are the specific security issues, threats,attacksand challenges facing patient in IoMT systems?

RQ2.2: What are the specific security issues, threats,attacks and challenges facing medical professionals in IoMT systems?

RQ2.3: What are the specific security issues, threats,attacks and challenges facing System administrator in IoMT systems?

RQ3: What are the specific security issues, threats,attacks and challenges facing IoMT Solution?

RQ4: What are the specific security issues, threats,attacks and challenges facing IoMT Architecture?

3.2. Search Stretegy:

This is an exceptionally critical iterative cycle to frame a string for searching. From the outset, we observed the SLR guidelines to make an entire string utilizing Boolean OR/AND [126]. The whole similar meanings of the said terms along with their alternatives are used with “OR” and then ended to establish searching string. To get the pertinent studies we applied the query string on well-known search engines such as Elsevier, IEEE, Springer, Science Direct, ACM Digital Library etc. Catchphrases from recently gotten ones and known essential examinations stayed involved in the string. Here, we analyzed the abstracts, titles, and creator expressions from a few notable fundamental investigations to recognize and look for terms.

3.3. Search Terms:

In the formation of the search query, keywords or index term play a vital role. We get the following key terms and their alternatives from the studies of well-known researchers as shown in Table No.1

3.3.1. Keywords Identification:

Here are the keywords categorized according to IoMT stakeholder, IoMT architecture, and IoMT solutions, along with some additional keywords:

Table-1: Keywords Identification

IoMT Stakeholder Keywords	
Category	**Keywords**
Patient Security	Patient data security, Data privacy, Data confidentiality, Informed consent, Patient safety
Medical Officials Security	Medical device security, Healthcare security, Cybersecurity threats, Clinical workflow
System Administration Security	Network security, Access control, Endpoint security, Device management, Patch management
Compliance	HIPAA compliance, GDPR compliance, Regulatory compliance, Standards, Best practices
IoMT Architecture Keywords	
Category	**Keywords**
Security Threats	Security threats, Cybersecurity threats, Malware, Ransomware, Phishing, Social engineering, Man-in-the-middle attacks

Network Security	Network security, Wireless security, Cloud security, Firewall, Intrusion detection, Intrusion prevention
Device Security	Device security, Mobile device security, Malware protection, Encryption, Decryption
Cloud Deployment	Cloud-based deployment, Security in the cloud, Cloud security best practices
On-premises Deployment	On-premises deployment, Security in on-premises environments, On-premises security best practices
IoMT Solutions Keywords	
Category	**Keywords**
Security Measures	Security measures, Risk assessment, Security controls, Security audits, Incident response
Compliance	Compliance solutions, HIPAA compliance, GDPR compliance, Regulations, Standards, Best practices
Threat Intelligence	Threat intelligence, Security education, Awareness training, Security culture, Penetration testing
Security Protocols	Authentication, Authorization, Access control, Encryption, Decryption

3.1.2. Search Query:

The expression "IoMT" has an extensive number of alike words and replace “3” terminologies that are used in literature and some of them have been enlisted in table-2. I studied allot of literature and included to my set of known studies more alternative terms for ‘Improving Security Architecture of Internet of Medical Things" were discovered. A single word (i.e. "IoMT") has been selected to get the majority of its conceivable inter-change terms, then ANDed it with "IoMT" to sift through totally unessential investigations from different areas. The study is further filtered by ANDing the terms “Security Issues”, “threats,attacksand challenges for Improving Security Architecture of Internet of Medical Things. The system of known basic studies was likewise utilized to evaluate the exactness of the inquiry string. The final search string has been displayed underneath. It should also be noted that the said string has to be altered in like manner for every one of the databases.

During this step, we identified the source bases and source strings that were utilized to choose the primary studies for our inquiry. The results of merging the several terms defining our research subject using the Boolean operators AND and OR to produce our research question are as follows**:**

Table-2: Search Query

IoMT Stakeholder	
Category	**Search Query**
Patient Security	"Patient data security" AND "IoMT security" OR "Data privacy" AND "healthcare security"
Medical Officials Security	"Medical device security" AND "healthcare security" OR "Cybersecurity threats" AND "clinical workflow"

System Administration Security	"Network security" AND "system administration" OR "Access control" AND "endpoint security"
Compliance	"HIPAA compliance" AND "patient data privacy" OR "GDPR compliance" AND "regulatory compliance"
IoMT Architecture	
Category	**Search Query**
Security Threats	"Security threats" AND "IoMT security" OR "Cybersecurity threats" AND "medical devices" OR "Ransomware"
Network Security	"Network security" AND "IoMT architecture" OR "Wireless security" AND "IoMT devices" OR "Cloud security"
Device Security	"Device security" AND "medical IoT" OR "Malware protection" AND "IoMT devices" OR "Encryption"
Cloud Deployment	"Cloud-based deployment" AND "IoMT security" OR "Cloud security best practices" AND "IoMT deployment"
On-premises Deployment	"On-premises deployment" AND "IoMT security" OR "On-premises security best practices" AND "IoMT solutions"
IoMT Solutions	
Category	**Search Query**
Security Measures	"Security measures" AND "IoMT security" OR "Security controls" AND "incident response" OR "Security audits"
Compliance	"Compliance solutions" AND "GDPR compliance" OR "Regulations" AND "best practices" OR "HIPAA compliance"
Threat Intelligence	"Threat Intelligence" OR "Security Education" OR "Awareness Training" AND "Security Culture" OR "Penetration Testing" OR "Security Education" OR "Awareness Training"
Security Protocols	"Authentication" AND "Authorization" AND "Access Control" OR "Encryption" AND "Encryption" AND "Decryption"

3.1.3. Online Databases:

The following table-3 shows the list of online databases where I have applied the search queries to retrieve relevant articles for my systematic literature review.

Table-3: Online Databases

Database Name	Description	Access Link
ACM Digital Library	A collection of full-text articles from ACM (Association for Computing Machinery) publications, including journals, conference proceedings, and	https://dl.acm.org/

	magazines.	
IEEE Xplore Digital Library	A database of full-text articles from IEEE (Institute of Electrical and Electronics Engineers) publications, including journals, conference proceedings, and standards.	https://ieeexplore.ieee.org/
ScienceDirect	A large database of full-text articles from various publishers in the fields of science, technology, medicine, including computer science.	https://www.sciencedirect.com/
SpringerLink	Database of full-text articles and book chapters from Springer publications, including journals, conference proceedings & books in computer science & related fields.	https://link.springer.com/
Scopus	A large abstract and citation database covering various fields, including computer science, engineering, and technology. It includes articles from scholarly journals, conference proceedings, and books.	https://www.scopus.com/
Web of Science	A multidisciplinary citation database that includes articles from scholarly journals, conference proceedings, and books in various fields, including computer science.	https://www.webofscience.com/
Other	Other Databases of full-text articles and book chapters from publications, including journals, conference proceedings & books in computer science & related fields.	Other Link Addresses

3.1.4. Primary and Secondary Search Strategies:

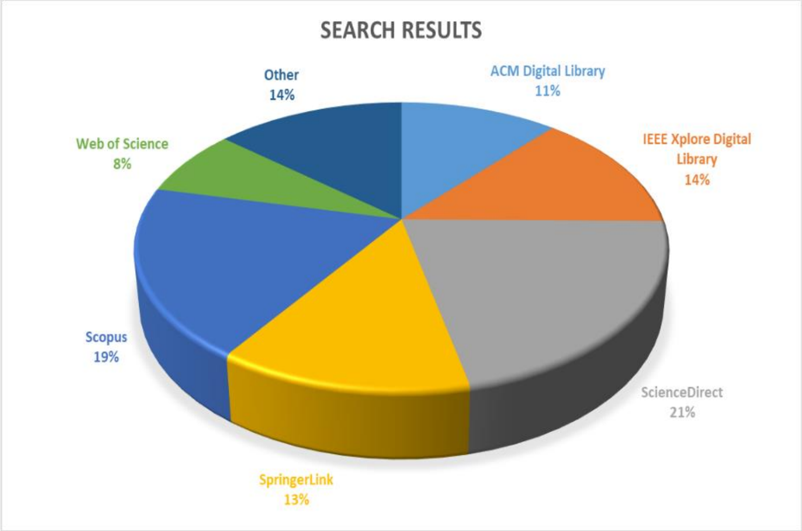
The following table-4 displays the number of articles retrieved from online databases before and after duplicate removal. The "Before Duplicate Removal" column indicates the number of articles retrieved from each database prior to removing duplicates, while the "After Duplicate Removal" column indicates the number of articles remaining after duplicates were removed. By providing this information, the table gives readers a sense of the size and scope of the initial literature search and the number of unique articles that were identified from each database.

Table 4: Search Results

Database Name	Before Duplicate Removal	After Duplicate Removal
ACM Digital Library	15	14
IEEE Xplore Digital Library	18	18
ScienceDirect	28	27

SpringerLink	17	17
Scopus	25	24
Web of Science	10	10
Other	18	17
Total	**131**	**127**

Figure – 1: Graphical Representation of Search Results



3.1.5. Study Selection Criteria:

The research question led to the establishment of inclusion and exclusion criteria as well as the goals of the systematic literature review (SLR). The subsequent step involved paper screening, which required the assessment of each article's eligibility based on specific inclusion and exclusion criteria. The goal was to retrieve only the most relevant studies that presented security issues, threats,attacks and challenges in the IoMT healthcare environment.

Inclusion Exclusion Criteria:

The inclusion criteria for the study selection include research that investigates security issues in IoMT systems, focuses on privacy concerns in IoMT, proposes solutions to address security challenges in IoMT, discusses the impact of emerging technologies on the security of IoMT, and analyzes the security risks associated with IoMT in the context of healthcare or other relevant domains. Moreover, studies that employ various research methods such as systematic reviews, surveys, case studies, or experiments are also considered.

On the other hand, the exclusion criteria comprise studies that do not focus on the security issues of IoMT, are not published in English, are not peer-reviewed, are not accessible in full-text format, are outdated or irrelevant (e.g., published before 2009), or are not related to healthcare or relevant domains.

3.1.6. Study Selection Process:

It was performed in the following Two stages. Which one is level screening, Title and Abstract, while the other is Quality Assessment (QA)

3.1.7. Level screening, Title and Abstract:

At this stage of the systematic literature review, the abstracts and titles of the 131 focused papers were managed. In order to determine the relevance of each paper, inclusion/exclusion criteria were applied to the abstracts and titles. Papers that were deemed not relevant to the research question or outside the scope of the review were excluded. For example, papers with titles containing the term "IoT Network" were excluded as they were outside the scope of the review. In some cases, the article's abstract was evaluated to determine whether the article was relevant or not. Papers that did not focus on security or did not present empirical data were also excluded. After screening the abstracts and titles, 94 papers were retained.

The full-text level screening involved a careful examination of each of the 94 papers, and inclusion criteria were applied to each of them. Thirteen papers were excluded at this stage. It was observed that some of the papers were of variable quality, with some being misleading or poorly written, and some providing little indication of what was in the full article. However, all papers that included some aspect of security were included in the review.

3.1.8. Quality Assessment:

As per the "13" criterion given in [15] as demonstrated in Table 5, each of the 94 papers were surveyed independently. Every single inquiry was responded to with "Yes" (Y=1), "No" (N=0), and the "average" (A=0.5) utilizing a 3-point scale and every study could get 0-13 facts. As the endpoint for including a review utilizing the primary quartile (13/3= 4.33). On the off chance, it would be chosen in any case eliminated that a review got more or equivalent to "4.33".

Table 5: Quality Assessment Checklist [15]

S. No	Question	Score
1.	Was the study designed to achieve these aims?	Y/N/ A
2.	Are the research aims clearly specified?	Y/N/ A
3.	Are the estimation techniques used clearly described and their selection justified?	Y/N/ A
4.	Are the variables considered by the study suitably measured?	Y/N/ A
5.	Are the data collection methods adequately described?	Y/N/ A
6.	Is the purpose of the data analysis clear?	Y/N/ A
7.	Is the data collected adequately described?	Y/N/ A
8.	Are statistical techniques used to analyze data adequately described and their use justified?	Y/N/ A
9.	Do the researchers discuss any problems with the validity/ reliability of their results?	Y/N/ A
10.	Are negative results (if any) presented?	Y/N/ A
11.	Are all research questions answered adequately?	Y/N/ A
12.	How clear are the links between data, interpretation and conclusions?	Y/N/ A
13.	Are the findings based on multiple projects	Y/N/ A

3.1.9. Results of SLR:

Table 6 shows the results of a systematic literature review (SLR) that began with an initial database search of 131 papers. Out of these one paper was unapproachable so we got 130. After abstracts and titles screening 36 papers were removed and the result was 94 papers. On the basis of inclusive/exclusive criteria on 94 papers we found 13 papers that were rejected. Out of remaining 81 papers, 4 papers were found identical study and were removed with having total numbers of 77 papers. 13 papers were rejected on the bases of quality assessment, leaving a final set of 64 papers for inclusion in the SLR. The cumulative total column shows the number of papers remaining at each stage of the SLR.

Table 6: Summary of Systematic Literature Review Results

Stage of SLR	Number of Papers	Cumulative Total
Initial database search	131	131
Unapproachable papers	1	130
After abstracts and titles screening	36	94
Omitted on inclusive/exclusive criteria	13	81
Identical studies	4	77
Rejected based on quality assessment	13	64
Final papers	**64**	

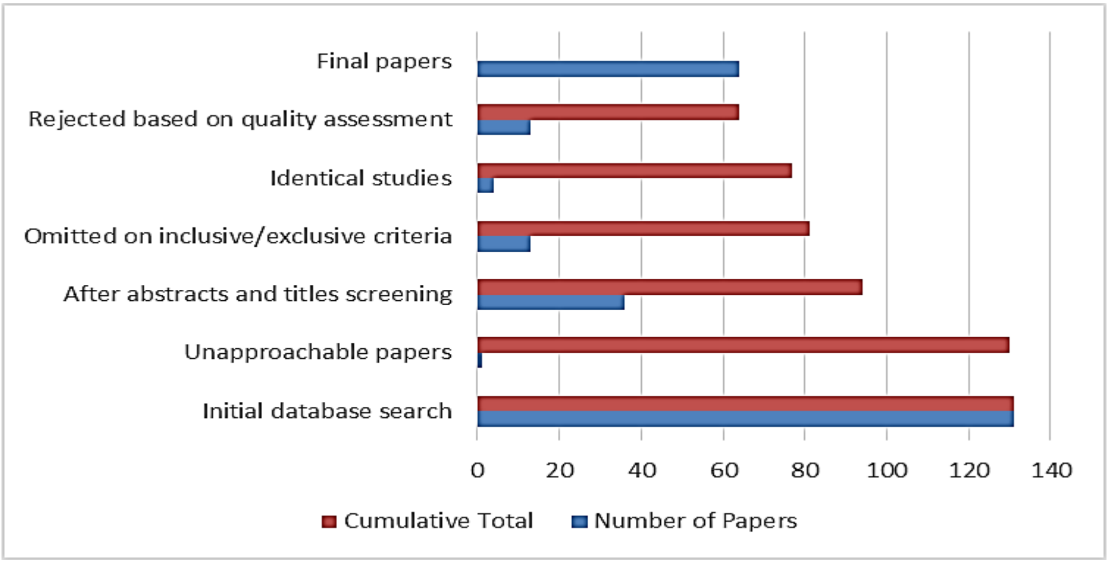


Figure – 2: Graphical Representation of Table - 6

3.1.10. Data Analysis for Research Questions:

Results of Research Questions:

This section presents the results of the systematic literature review (SLR) in relation to the research questions of the study. The SLR aimed to identify and synthesize existing research on a research question, and the results are presented here in a way that addresses each research question in turn. The findings related to each research question are presented and discussed, with a focus on the most significant and relevant results. The results are supported by data from the included studies, as well as any relevant tables or figures. By presenting the results in this way, readers can easily understand how the SLR addressed the research questions and what the key findings were. The results section is an important part of any SLR, as it provides a clear and comprehensive summary of the most relevant and significant research in the field.

How to improve the Security Architecture of IoMT?(RQ1)

The main key to improve the Security Architecture of IoMT is to identify, prioritize and handle most of the security issues , threats , attacks and challenges that mayeffect the security and privacy of all stakeholders , solution and architecture of Internet of Medical Things. Moreover RQ2,RQ3 and RQ4 address most of the Security Issues , Threats, Attacks and Challenges to improve the security architecture of Internet of medical things.

Patient Security Issues/Threats/Attacks/Challenges: (RQ 2.1)

Patients are a critical stakeholder in the Internet of Medical Things (IoMT) ecosystem, and their personal health data is one of the most valuable assets that need to be protected. Patients are also primary users of IoMT devices and services, and they are directly affected by any security incidents or breaches.

For example, unauthorized access to personal health data, inadequate authentication and authorization mechanisms, and insufficient encryption of sensitive data can all put patients' health information at risk. Malware and ransomware attacks, physical tampering and theft of devices, and social engineering attacks targeting patients can cause harm to patients and disrupt medical treatment.

Therefore, it is essential to identify and address security issues/threats/attacks/challenges that affect patients in IoMT to ensure their safety and privacy.

Hence for String Searching I have developed my own tool to identify different security issues, threats,attacks and challenges affecting stockholders, solutions and architecture of IoMT

Following Tables are the categorical representation of security issues, threats,attacks and challenges affecting stockholders, solutions and architecture of IoMT.

Table: 7 Security Issues/Threats/Attacks/Challenges of Patients

S. No.	Category	Security Issue / Threat / Attack/ Challenge	Description	Frequency	%
1	Ethical	Ethical concerns around patient data use and ownership	Ethical concerns regarding the use and ownership of patient health data	45	70.31
2	Data Privacy	Unauthorized access to personal health data	Access to patient health data without proper authorization	43	67.19
3	Cyberattacks	Cyberattacks on medical facilities and systems	Cyberattacks on medical facilities, including hospitals, clinics, and medical data centers	42	65.63
4	Testing and Validation	Inadequate security testing and validation	Inadequate security testing and validation of IoMT devices and systems	42	65.63
5		Lack of transparency in data collection and use	Lack of transparency in how patient data is collected, used, and shared	38	59.38
6	Safety	Interference with medical device functionality	Interference with the functionality of IoMT devices, causing harm to patients	36	56.25
7	Lifecycle	Lack of device	Inadequate management of	36	56.25

	Management	and data lifecycle management	the lifecycle of IoMT devices and health data		
8	Mobile Security	Insecure mobile applications for IoMT devices	Security vulnerabilities in mobile applications used to control IoMT devices	35	54.69
9	Application Security	Inadequate security testing of IoMT applications	Inadequate security testing of applications used in IoMT devices and systems	34	53.13
10	Disaster Recovery	Lack of disaster recovery plans	Inadequate disaster recovery plans for IoMT devices and systems	33	51.56
11	Cloud Security	Security risks associated with the cloud	Security risks associated with cloud based IoMT solutions and services	32	50.00
12		Limited standardization and regulation of IoMT devices	Limited standardization and regulation of IoMT devices	31	48.44
13	Legacy Systems	Security risks associated with legacy devices and systems	Security risks associated with legacy IoMT devices and systems	31	48.44
14		Inadequate physical security of devices	Inadequate physical security measures for IoMT devices, including theft, loss, and damage	30	46.88
15	Legal and Regulatory	Lack of accountability and liability for security breaches	Lack of clear accountability and liability for IoMT security breaches	30	46.88
16	Social Engineering	Social engineering attacks targeting patients	Manipulation of patients through deceptive tactics	29	45.31
17		Unsecured remote access to IoMT devices	Insecure remote access to IoMT devices	28	43.75
18	Software Security	Vulnerabilities in IoMT device software and firmware		28	43.75
19		Denial-of-service attacks on medical networks	Overwhelming medical networks with traffic to disrupt services	27	42.19
20		Insecure data storage and management practices	Inadequate data storage and management policies and practices	27	42.19

21		Inadequate monitoring of network traffic	Inadequate monitoring of network traffic for IoMT devices and systems	26	40.63
22	Malware	Malware and ransomware attacks on IoMT devices	Malicious software that can infect and compromise IoMT devices	26	40.63
23		Unauthorized sharing of personal health data	Unauthorized sharing of patient health data without proper consent	26	40.63
24	Risk Management	Difficulty in identifying and mitigating IoMT security risks	Difficulty in identifying and mitigating IoMT security risks	25	39.06
25		Security risks associated with outdated devices and software	Security risks associated with outdated IoMT devices and software	25	39.06
26	Supply Chain	Compromised supply chains for medical devices	Security risks associated with compromised supply chains for IoMT devices	24	37.50
27		Interference with IoMT device firmware updates	Interference with IoMT device firmware updates, potentially compromising security	24	37.50
28	Physical Security	Physical tampering and theft of devices	Physical theft or tampering of IoMT devices	12	18.75
29	Data Integrity	Interference with medical data accuracy and integrity	Interference with the accuracy and integrity of patient health data	12	18.75
30		Lack of timely security updates and patches	Failure to provide timely security updates and patches for IoMT devices	12	18.75
31		Inadequate risk assessment and management	Inadequate risk assessment and management for IoMT devices and systems	12	18.75
32	Third-Party Risk	Security risks associated with third-party services	Security risks associated with third-party services used in IoMT systems	12	18.75
33	Logging and Monitoring	Insufficient device monitoring and	Inadequate monitoring and event logging for IoMT devices	12	18.75

		event logging			
34		Unauthorized modification of device settings	Unauthorized modification of settings on IoMT devices	12	18.75
35	Network Security	Lack of secure communication protocols between devices	Vulnerable communication channels between IoMT devices	12	18.75
36	Access Control	Inadequate authentication and authorization mechanisms	Weak or nonexistent authentication and authorization processes	12	18.75
37	Insider Threats	Insider threats from employees or contractors	Threats to IoMT security from insiders, including employees and contractors	12	18.75
38	Data Protection	Insufficient encryption of sensitive data	Lack of proper encryption for sensitive health data	12	18.75
39	Integration	Lack of integration with existing security solutions	Lack of integration with existing security solutions, resulting in potential security gaps	12	18.75

Medical Professional Security Issues/ Threat / Attack/Challenge: (RQ2.2)

The following table-8 shows the frequency and percentage of each security issue related to medical officials in IoMT identified in the SLR.

Table - 8: Medical Professional Security Issues/ Threat /Attack/ Challenge

S. No	Category	Security Issue / Threat / Attack/ Challenge	Description	Frequency	%
1	Data Privacy	Unauthorized access to patient data	Unauthorized access to patient data stored on IoMT devices or transmitted over networks	56	87.50
2	Training and Awareness	Insufficient security training	Insufficient security training for medical officials using IoMT devices and systems	47	73.44
3	Disaster Recovery	Inadequate data backup and recovery	Inadequate data backup and recovery for IoMT devices and systems, potentially resulting in data loss	46	71.88
4	Insider Threat	Insider threats	Insider threats from employees or contractors with authorized access to patient data	45	70.31
5	Communication Security	Insecure communication channels	Insecure communication channels used to transmit sensitive patient data	43	67.19
6	Access Control	Lack of access controls	Lack of access controls to limit access to sensitive patient data	40	62.50

7	Malware	Malware infections	Malware infections of IoMT devices, potentially compromising patient data	38	59.38
8	Software Security	Inadequate software updates	Inadequate software updates for IoMT devices, potentially leaving them vulnerable to attacks	35	54.69
9	Data Security	Insufficient data encryption	Insufficient encryption of patient data, making it vulnerable to interception and theft	33	51.56
10	Authentication	Lack of device authentication	Lack of device authentication, allowing unauthorized devices to access sensitive patient data	33	51.56
11	DDoS	Distributed denial-of-service (DDoS) attacks	DDoS attacks on IoMT systems, potentially disrupting patient care	30	46.88
12	Risk Management	Inadequate risk management	Inadequate risk management for IoMT devices and systems, potentially leaving them vulnerable to attacks	28	43.75
13	Device Functionality	Interference with device functionality	Interference with IoMT device functionality, potentially compromising patient care	25	39.06
14	Third-Party Risk	Lack of vendor security oversight	Lack of security oversight of third-party vendors providing IoMT devices and services	22	34.38
15	Business Continuity	Lack of contingency planning	Lack of contingency planning for IoMT devices and systems, potentially disrupting patient care	19	29.69
16	Physical Security	Physical security breaches	Physical security breaches, such as theft or tampering of IoMT devices	16	25.00
17	Decision-Making	Inadequate security controls for clinical decision-making	Inadequate security controls for clinical decision-making using IoMT devices and data	15	23.44
18	Interoperability	Inadequate security controls for medical device interoperability	Inadequate security controls for medical device interoperability, potentially compromising patient care	13	20.31

System Administration Issues / Threats / Attacks/Challenges: (RQ2.3)

The following table-9 represents the security issues related to System administrators. These issues are identified from the findings of SLR.

Table - 9:System Administrator's Issues

S. No	Category	Security Issue / Threat / Attack/ Challenge	Description	Frequency	%
1	Privacy Privacy	Unauthorized Access	Unauthorized access to sensitive medical data, such as personal health information (PHI) and electronic health records (EHRs).	45	70.31
2		Data leakage	Data leakage can occur due to misconfigured systems or devices, unauthorized access, or malicious insiders, leading to the loss of sensitive data.	28	43.75
3	Authentication	Weak authentication mechanism	Weak authentication mechanisms, such as easily guessable passwords or insufficiently secure authentication protocols.	44	68.75
4	Data	Data loss	Loss of data due to system failure, cyber-attack or natural disasters.	43	67.19
5	Cyber Attacks	Distributed denial-of-service (DDoS) attacks	DDoS attacks can cause system downtime, leading to service disruption, and in the case of IoMT devices, can result in life-threatening situations.	41	64.06
6		Malware and ransomware attacks	Malware, ransomware, and other cyber-attacks can lead to data breaches, data destruction, and unauthorized access to medical devices or networks.	40	62.50
7		Cyberterrorism	Cyberterrorism involves the use of cyber-attacks to cause harm to individuals, organizations, or governments, and can have severe consequences for the healthcare sector.	28	43.75
8	Integrity	Data tampering	Modification or tampering of data, leading to inaccurate medical diagnoses or incorrect treatment.	38	59.38
9	Authorization	Insufficient user permissions	Insufficient user permissions, which can lead to unauthorized access to sensitive data or inappropriate system usage.	37	57.81

10	Social Engineering	Phishing attacks	Cybercriminals can use phishing attacks to trick medical officials into providing sensitive information or clicking on malicious links.	36	56.25
11		Social media threats	Medical officials and system administrators may unintentionally disclose sensitive information or fall victim to social media attacks such as phishing or social engineering.	14	21.88
12		Baiting attacks	Baiting attacks target medical officials by offering a reward or incentive in exchange for sensitive information or access to critical systems.	32	50.00
13		Pretexting attacks	Pretexting attacks involve cybercriminals impersonating someone else, such as a medical official or IT staff, to gain access to sensitive information or systems.	32	50.00
14	Insider Threats	Insider threats	Insiders, such as system administrators or medical professionals, can pose a threat to sensitive data or critical systems.	34	53.13
15		Insider trading	Insider trading involves the exploitation of confidential information for financial gain & can have severe consequences for medical officials or organizations.	34	53.13
16	Interoperability	Incompatibility or inability to communicate	Incompatibility or inability to communicate with other systems or devices, which can hinder information sharing and collaboration among medical officials.	32	50.00
17	Data Protection	Lack of encryption	Lack of encryption for sensitive data can leave it vulnerable to interception or unauthorized access.	31	48.44

18	Business Continuity	Lack of backup and recovery	Lack of proper backup & recovery mechanisms can lead to data loss & in case of a disaster, system downtime & business continuity issues.	29	45.31
19	System Configuration	Misconfiguratio n	Misconfigurations of IoMT devices & systems can leave them vulnerable to attack or unauthorized access.	28	43.75
20	Access Control	Insufficient access control	Lack of proper access controls for critical systems and data, leading to unauthorized access and potential data breaches.	26	40.63
21	Risk Management	Failure to perform risk assessments	Failure to perform regular risk assessments can lead to unidentified security vulnerabilities or threats.	25	39.06
22	Regulatory Compliance	Non-compliance with regulations	Non-compliance with regulatory requirements and standards, such as HIPAA or GDPR, can lead to penalties and legal actions against medical officials or organizations .	24	37.50
23	System Maintenance	Failure to update systems	Failure to apply security patches and updates in a timely manner can leave systems vulnerable to known security vulnerabilities.	23	35.94
24	Physical Security Physical Security	Theft of IoMT devices	Theft of IoMT devices can lead to unauthorized access to sensitive data and potential data breaches.	21	32.81
25		Lack of physical security	Lack of physical security measures, such as surveillance cameras, access controls, or alarms, can lead to theft or unauthorized access to critical systems or data.	15	23.44
26	Third-Party Risks	Third-party vendor risks	Third-party vendors with access to critical systems or data can pose a security	18	28.13
27	Security Monitoring	Lack of security monitoring	Lack of proper security monitoring tools and practices can lead to delayed detection of security incidents or data breaches.	15	23.44

IoMT Solutions Issues/Threats/Attacks and Challenges (RQ3)

The following table-10 shows security issues related to IoMT solutions, extracted from SLR.

Table- 10:IoMT Solutions Issues

S. No	Category	Security Issue / Threat / Attack/ Challenge	Description	Frequency	%
1	Interoperability	Interoperability issues	IoMT solutions may use different communication protocols, making it difficult for devices and systems to communicate with each other	47	73.44
2	Scalability	Scalability issues	Managing and securing a large number of connected medical devices and sensors can be challenging due to limited resources, network congestion, and other factors	46	71.88
3	Data security	Data breaches	Unauthorized access to sensitive patient data during storage or transmission	45	70.31
4		Lack of encryption	Insufficient or ineffective encryption of patient data during transmission	40	62.50
5	System security	Malware attacks	Introduction of malware into IoMT systems through various means, such as phishing attacks or infected software updates	43	67.19
6	System security	Insider threats	Intentional or unintentional security breaches by employees or contractors with authorized access to IoMT systems	34	53.13
7	User error	User error	Weak passwords or failure to update software can compromise the security of IoMT devices and systems	41	64.06
8	Complexity	Complexity of IoMT systems	IoMT solutions can be complex and difficult to manage, especially for healthcare organizations with limited IT resources	40	62.50
9	Liability	Liability issues	Liability issues may arise if patients are harmed due to a security breach or malfunction of an IoMT device	37	57.81
10	Ethical concerns	Ethical concerns	The use of IoMT solutions raises ethical concerns related to patient privacy, data ownership, and the potential for unintended consequences, such as	34	53.13

			algorithmic bias		
11	Regulatory compliance	Compliance issues	Non-compliance with regulatory requirements, such as HIPAA and GDPR, to ensure patient data privacy and security	28	43.75

IoMT Architecture Issues/Threats/Attacks/Challenges (RQ4)

The following table-11 represents the security issues related to IoMT architecture.

Table – 11:IoMT Architecture Issues

S. No	Category	Security Issue / Threat / Attack/ Challenge	Description	Frequency	%
1	Technical	Interoperability	Difficulty in integrating various IoMT devices from different manufacturers and different standards, resulting in compatibility issues and hindering data sharing and analysis.	48	75.00
2		Connectivity	Weaknesses in wireless network infrastructure and coverage, leading to loss of data and limited range of IoMT devices.	45	70.31
3		Device Management	The complexity of managing large numbers of IoMT devices, including device configuration, software updates, and patch management.	42	65.63
4		Cybersecurity	The risk of unauthorized access to and manipulation of sensitive medical data, as well as the possibility of ransomware attacks that disrupt medical services.	40	62.50
5	Ethical	Privacy	The potential violation of patient privacy due to the collection and use of sensitive medical data by IoMT devices, and the risk of data breaches and leaks.	44	68.75
6		Autonomy	The loss of patient autonomy and control over their own medical data and treatment due to the reliance on IoMT devices and the algorithms that drive them.	41	64.06

7	Social	Access and Equity	Unequal access to IoMT devices and services due to cost and availability, as well as potential disparities in quality of care and health outcomes.	39	60.94
8	Regulatory	Compliance	The need to comply with various regulatory requirements and standards, such as HIPAA, FDA regulations, and GDPR, to ensure patient data privacy and security.	37	57.81

4. Conclusion:

This study presents a comprehensive approach to address the security challenges facing IoMT stakeholders, solutions, and architecture. As IoMT adoption grows in healthcare, maintaining confidentiality, integrity, and availability of patient data while protecting against threats is crucial. This research contributes to IoMT security by providing a practical approach to enhancing patient data privacy and security. It identifies security issues and educates stakeholders on IoMT security, promoting transparency and accountability. The main goal is to improve IoMT's security architecture, benefiting adopters and future researchers who aim to enhance existing models or develop new ones. However, further research is needed to develop specific guidelines and best practices for addressing IoMT security challenges.

References

[1]. F. Alsubaei, A. Abuhussein, and S. Shiva, “Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment,” IEEE Xplore, pp. 112-120, Oct. 01, 2017. https://ieeexplore.ieee.org/document/8110212

[2]. M. S, S. Almutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan, and R. Patan, “Effective Attack Detection in Internet of Medical Things Smart Environment using a Deep Belief Neural Network,” IEEE Access, pp. 77396-77404, 2020, doi:https://doi.org/10.1109/access.2020.2986013

[3]. M. Irfan and N. Ahmad, “Internet of medical things: Architectural model, motivational factors and impediments,” 2018 15th Learning and Technology Conference (L&T), pp. 6-13, Feb. 2018,doi: https://doi.org/10.1109/lt.2018.8368495

[4]. G. J. Joyia, R. M. Liaqat, A. Farooq, and S. Rehman, “Internet of Medical Things (IOMT): Applications, Benefits and Future Challenges in Healthcare Domain,” Journal of Communications, vol. 12, no. 4, pp. 240-247, 2017, doi: https://doi.org/10.12720/jcm.12.4.240-247

[5]. X. Li, H.-N. Dai, Q. Wang, M. Imran, D. Li, and M. A. Imran, “Securing Internet of Medical Things with Friendly-jamming schemes,” Computer Communications, Jun.pp.431-442, 2020, doi: https://doi.org/10.1016/j.comcom.2020.06.026.

[6]. F. Al-Turjman, M. H. Nawaz, and U. D. Ulusar, “Intelligence in the Internet of Medical Things era: A systematic review of current and future trends,” Computer Communications, vol. 150, pp. 644–660, Jan. 2020, doi: https://doi.org/10.1016/j.comcom.2019.12.030.

[7]. P. P. Ray, D. Dash, and N. Kumar, “Sensors for internet of medical things: State-of-the-art, security and privacy issues, challenges and future directions,” Computer Communications, vol. 160, pp. 111–131, Jul. 2020, doi: https://doi.org/10.1016/j.comcom.2020.05.029.

[8]. Z. Guan, Z. Lv, X. Du, L. Wu, and M. Guizani, “Achieving data utility-privacy tradeoff in Internet of Medical Things: A machine learning approach,” Future Generation Computer Systems, vol. 98, pp. 60–68, Sep. 2019, doi: https://doi.org/10.1016/j.future.2019.01.058.

[9]. X. Huang and S. Nazir, "Evaluating Security of Internet of Medical Things Using the Analytic Network Process Method," Security and Communication Networks, vol. 2020, pp. 1–14, Sep. 2020, doi: https://doi.org/10.1155/2020/8829595.

[10]. I. S. Farahat, A. S. Tolba, M. Elhoseny, and W. Eladrosy, "A secure real-time internet of medical smart things (IOMST)," Computers & Electrical Engineering, vol. 72, pp. 455–467, Nov. 2018, doi: https://doi.org/10.1016/j.compeleceng.2018.10.009.

[11]. M. Papaioannou et al., "A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT)," Transactions on Emerging Telecommunications Technologies, Jul. 2020, doi: https://doi.org/10.1002/ett.4049.

[12]. M. Seliem and K. Elgazzar, "BIoMT: Blockchain for the Internet of Medical Things," 2019 IEEE International Black Sea Conference on Communications and Networking, pp.1-4, Jun. 2019, doi: https://doi.org/10.1109/blackseacom.2019.8812784.

[13]. F. Alsubaei, A. Abuhussein, and S. Shiva, "Ontology-Based Security Recommendation for the Internet of Medical Things," IEEE Access, vol. 7, pp. 48948–48960, 2019, doi: https://doi.org/10.1109/access.2019.2910087.

[14]. F. Alsubaei, A. Abuhussein, V. Shandilya, and S. Shiva, "IoMT-SAF: Internet of Medical Things Security Assessment Framework," Internet of Things, vol. 8, p. 100123, Oct. 2019, doi: https://doi.org/10.1016/j.iot.2019.100123.

[15]. B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering – A systematic literature review," Information and Software Technology, vol. 51, no. 1, pp. 7–15, Jan. 2009,
doi: https://doi.org/10.1016/j.infsof.2008.09.009