IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 10 May 2023, accepted 29 May 2023, date of publication 31 May 2023, date of current version 5 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3281655

TOPICAL REVIEW

Improving Security Architecture of Internet of Medical Things: A Systematic Literature Review

MUDASIR MAHMOOD[1], MUHAMMAD IJAZ KHAN[1], ZIAUDDIN[1], HAMEED HUSSAIN[2], INAYAT KHAN[3], SHAHID RAHMAN[2], MUHAMMAD SHABIR[2], AND BADAM NIAZI[4]

[1]Institute of Computing and Information Technology, Gomal University, Dera Ismail Khan 29050, Pakistan
[2]Department of Computer Science, University of Buner, Buner, Khyber Pakhtunkhwa 19290, Pakistan
[3]Department of Computer Science, University of Engineering and Technology, Mardan, Mardan 23200, Pakistan
[4]Faculty of Computer Science, Nangarhar University, Jalalabad 2660, Afghanistan

Corresponding author: Badam Niazi (badam@nu.edu.af)

ABSTRACT Ever since its emergence, the concept internet of things (IoT) has been applied in many fields. In the area of medical sciences, a new concept ''Internet of Medical Things'' (IoMT) has been explored. IoMT establishes a connection between humans & machines and serves both of them. It has been expected that, by 2025, services of IoMT would reach the entire world. IoMT has covered a wide scope pertaining to health but unfortunately been facing many security challenges. Healthcare systems consist of sensitive and significant data, which is unorganized and noisy and needs additional power to be calculated for effective analysis & workable results. This data is worked upon for the purpose of making critical decisions. Therefore, it has become the main target of Cyber Criminals. The need of robust security and privacy (S&P) is gradually increasing as more and more devices are getting connected to the IoMT. The S&P of the IoMT has now become a great challenge, considering the utmost significance and vulnerability of the data in the healthcare industry. Lack of sufficient S&P in IoMT devices keeps the patient' privacy at high stake. This research is intended to propose a Security Model to cope with these Security threats, attacks, issues and challenges. The proposed model has been developed by thoroughly investigating all the major security models through a detailed systematic literature review. The SLR has been conducted to explore all the security threats, security attacks, security issues and security challenges. Extensive meta-analysis has been performed for each of the defined category in order to prioritize these risks. After analyzing these risks, a comprehensive security model has been proposed. The interface has been developed in Python which is well structured, user friendly and easy to implement. The developed module not only identify and prioritize the risks but also automatically control different level of threats. The developed system also contain user intimation modules in case of any threat. This research is based on a very flexible and comprehensive model, which would be highly beneficial to future researchers who desire to work on existing models for the improvement as well as to those who wish to create new security models for IoMT.

INDEX TERMS Internet of Medical Things, security, issues, healthcare, privacy, IoT, stakeholder.

I. INTRODUCTION

Sensors, as a tool of smart healthcare, are very important smart devices that measure heart rate, blood pressure, sleep patterns, body temperature, brain activity and other data related to health [S1]. 1/3rd of the IoT the devices are available for health care at present which are expected to rise by 2025 for approx. 40 percent having the global financial value of Internet of Things technology i-e $6.2 trillion [S2]. IoMT provides solutions to the problems faced by outdated medical systems like lack of health care resources, doctors whereas, the research data collected through IoMT may be used by researchers to diagnose and predict diseases [S3]. It measures the vital signs of patients to store on the cloud

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamed Elhoseny.

by aggregating them into medical data files so that healthcare workers may access them [S4]. Regular monitoring of patients and elder people via wearable devices and sensors gained attention. The goal includes monitoring blood pressure, temperature and heart rates which are important for toda's world healthcare, Need of the day is remote real-time healthcare monitoring to address all these challenges [S5]. IoMT brings some improvements in lives of patients in clinician's work and health system's economy [S6].

The devices of Internet of Medical Things are detailed in network by not keeping in mind the security issues, threats and attacks. Resultantly, the cybercriminals get access into the IoMT network and reach the IoMT network and receive the really sensitive and recorded personal data of the patients. Among the gravest problem facing IoMT devices includes security issues, threats and attacks in IoMT. Johnson and Johnson says, digital insulin is exposed to cyber threats [S7]. In order to ensure uninterrupted communication of these devices and to run them efficiently and effectively, their security is of utmost importance. Security of devices is indeed the protection from unauthorized access by illegal users. IoMT plays an important function, remotely, in the exchange of data processes. Internet of things devices have less capability because of low processing, limited storage, and tiny memory hence security implementation is a challenging task [S4]. The largest ransomware attack on medical systems had been reported in 2017 containing over 20 thousand devices across the globe. The lack of robust security that causes such attacks in the IoMT is because of multiple reasons. The complexity and incompatibility factors that result from the multifarious IoMT technologies, having inherent insecurity, i. e wireless sensor network and cloud, popped up various security issues [S2]. With technological evolution, the IoMT is more practical and doable in order to establish compelling control over wide range of tools to working so that health-related issues are not only identified but also rectified. Internet of Medical Things devices offers various aids. Further, they put security issues, threats and attacks related to privacy which are life-threatening [S8].

This study objectives are to Improve researchers understanding of the security issues, attacks and threats to IoMT networks.Its protective measures to provide a framework for planning research activities aimed at designing and creating appropriate lightweight security mechanisms that can overcome the resource and computing power constraints of IoMT devices and maintain network security.

A. SECTION AREA

This paper is organized into different sections: section II provides Motivation, a general introduction to IoMT, the state of the art, and (S &P) terminology for IoMT is provided in this section for motivation, section III describes a Systematic Literature Review, the technique by which the primary studies were arbitrarily chosen for analysis, section IV presents results as the findings of all the primary studies that were chosen, and Section V discusses the research questions findings. Section VI offers suggestions for improvement in the direction of a comprehensive strategy to protect against security Issues, Threats and Attacks to keep strong IoMT Architecture. Section VII is wrapped with the conclusion of our whole study about addressing security issues, threats and attacks to improve the Security Architecture of Internet of Medical Thing.

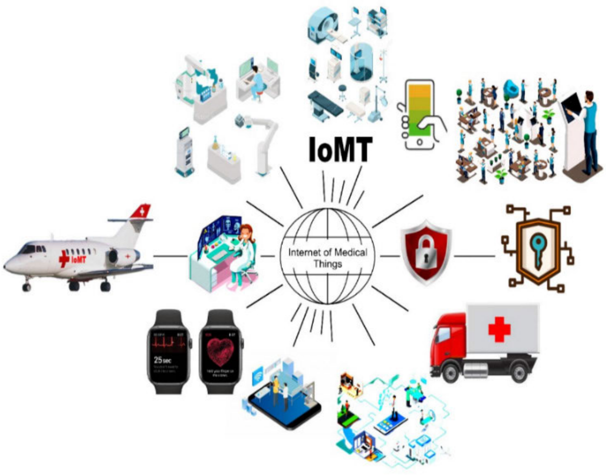


FIGURE 1. Internet of medical things.

II. MOTIVATION

IoMT is based on IoT for monitoring healthcare-related vital signs such as ECG, Heart Rate, Blood Pressure, Body Temperature, Pulse Rate, Oxygen Saturation, and Blood Glucose, Testing for Drug Abuse, Cholesterol Testing, Infectious Diseases, and Pregnancy. It is primarily responsible for providing quality life to patients without their need to be hospitalized. It ensures the care of patients inside and outside the hospital environment.

The network is the key component of IoMT having all IoMT-enabled devices which continuously oversee patients' health digitally e.g they can access their health status simply using a mobile phone or radio-frequency identification "RFID". These devices of IoMT include smart watches or smart shoes and also ECG sensors, airflow sensors, etc

Cybercriminals have left no stone unturned to disrupt the security in healthcare. In the past five years, the IoMT has been the target of several cyberattacks e.;

- In 2021, Cybercriminals heavily targeted the institutional servers of 1 CF Witting Hospital in Bucharest by ransomware attack.
- Similarly, the same attacks happened in 2019 at four other hospitals in Romania.
- In Italy, similar attacks were recorded that disrupted the vaccination schedule of several tertiary care hospitals in 2021
- Attackers can utilize stolen data for ransomware attacks, as happened in 2018 with an Indiana hospital

when medical records were encrypted. The hospital had to pay $50,000 to get the data back after the inciden

- The interruption of medical services is another type of ransomware assault, which may need expensive repairs. In order to restore vital services, Hollywood Presbyterian Medical Center was had to pay $17,000 in ransom in 2016
- In fact, the worst ransomware assault on medical systems ever recorded affected over 200,000 devices globally, including those in the United States
- IoMT attacks may also harm brand reputation, business continuity, and financial stabilit; therefore they have negative repercussions beyond just data loss and decreased patient well-being.
- The successes of such attacks and the weak security in the IoMT are caused by a variety of factors [S9]
- Therefore, a comprehensive, workable, secure and effective study about the Security issues, threats and attacks for the improvement of IoMT architecture has become a need of the time, which can repel the attackers and raise the level of trust of the patients.

III. 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.

A. KEY APPROACH USED IN THIS STUDY ARE DISCUSSED AS UNDER

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, attacks and challenges facing IoMT Stakeholders?

RQ2.1: What are the specific security issues, threats, attacks and 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?

RQ5: How to devise an implantable strategy to effectively implement the developed security framework in practical environment?

RQ6: How to motivate and train different stakeholders to comprehend and operate the implemented framework?

2) QUERY STRING

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 [123]. 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) 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

4) KEYWORDS IDENTIFICATION

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

5) 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 No.4.2. 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, attacks and 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 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

6) ONLINE DATABASE

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

7) PRIMARY AND SECONDARY SEARCH STRATEGIES

The following table displays the number of articles retrieved from online databases before and after duplicate removal. The "Before Duplicate Removal" column indicates the number

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"

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

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 magazines.	https://dl.acm.org/
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

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.

8) STUDY SELECTION CRITERI

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.

i. Inclusion Criteria:

- Studies that investigate security issues in IoMT systems
- Studies that focus on privacy concerns in IoMT
- Studies that propose solutions to address security challenges in IoMT
- Studies that discuss the impact of emerging technologies on the security of IoMT

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**

TABLE 5. Quality assessment checklist [123].

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

- Studies that analyze the security risks associated with IoMT in the context of healthcare or other relevant domains.
- Studies that use various research methods such as systematic reviews, surveys, case studies, or experiments.

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**	

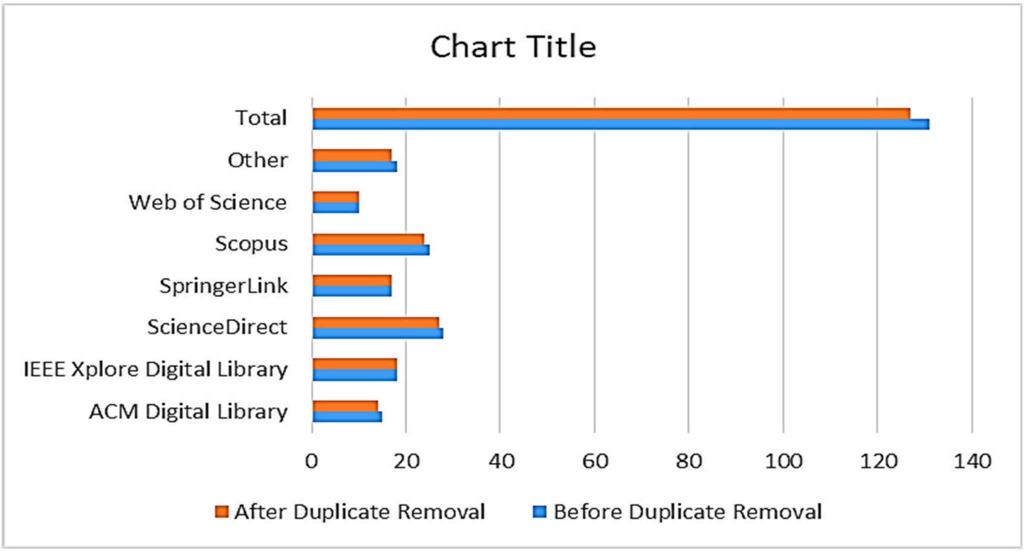


FIGURE 2. Graphical representation of search results.

ii. Exclusion Criteria:

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

9) STUDY SELECTION PROCES

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

i. 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.

ii. Quality Assessment As per the "13" criterion given in [123] as demonstrated in Table 5, each of the 94 papers were surveyed independently. Every single inquiry was

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 Management	Lack of device and data lifecycle management	Inadequate management of the lifecycle of IoMT devices and health data	36	56.25
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

TABLE 7. *(Continued.)* Security issues/threats/attacks/challenges of patients.

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

TABLE 7. *(Continued.)* Security issues/threats/attacks/challenges of patients.

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 event logging	Inadequate monitoring and event logging for IoMT devices	12	18.75
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

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

TABLE 8. *(Continued.)* **Medical professional security issues/ threat / attack/ challenge.**

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

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".

IV. RESULTS OF SLR

Table 4.6 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.

A. DATA ANALYSIS FOR RESEARCH QUESTIONS

1) 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.

a: 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 may effect the security and privacy of all stakeholders, solution and architecture of Internet of Medical Things. Moreover RQ2,RQ3,RQ4,RQ5 and RQ6 address most of the Security Issues, Threats, Attacks and Challenges to improve the security architecture of Internet of medical things.

b: 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.

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	36	56.25

TABLE 9. ***(Continued.)*** **System administrator's issues.**

			sensitive information or clicking on malicious links.		
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	Misconfiguration	Misconfigurations of IoMT devices & systems can leave	28	43.75

TABLE 9. *(Continued.)* System administrator's issues.

			them vulnerable to attack or unauthorized access.		
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

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 challenge 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.

c: MEDICAL PROFESSIONAL SECURITY ISSUES/THREAT/ATTACK/CHALLENGE: (RQ2.2)

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

d: SYSTEM ADMINISTRATION ISSUES/THREATS/ATTACKS/CHALLENGES: (RQ2.3)

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

TABLE 10. IoMT solutions issues.

S. No	Category	Security Issue / Threat / Attack/ Challenge	Description	Frequency	%
1	Interoperability	Interoperabilit y 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 algorithmic bias	34	53.13
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

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

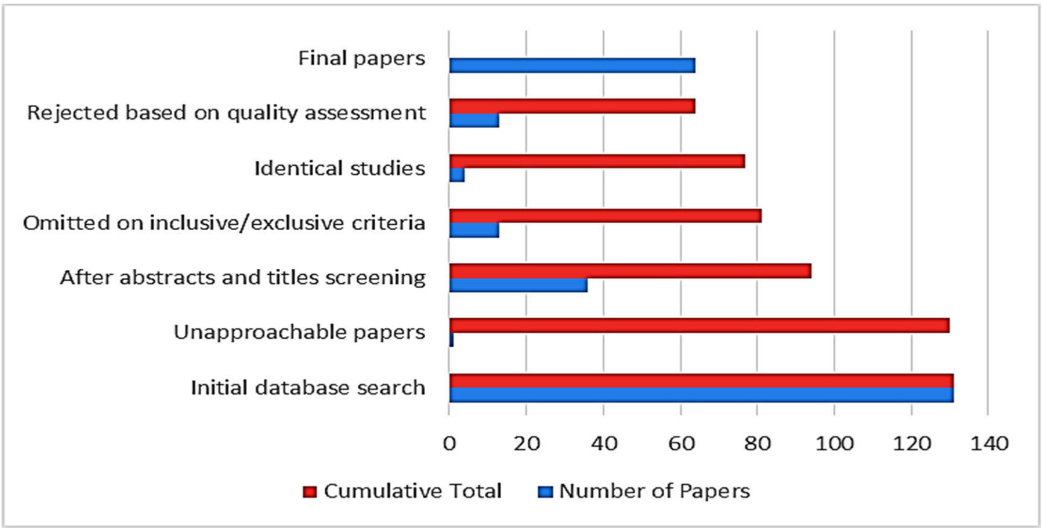


FIGURE 3. Graphical representation of Table - 6.

e: IOMT SOLUTIONS ISSUES/THREATS/ATTACKS AND CHALLENGES (RQ3)

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

f: IOMT ARCHITECTURE ISSUES/THREATS/ATTACKS/CHALLENGES (RQ4)

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

V. RESEARCH METHODOLOGY

The Internet of Medical Things (IoMT) is a rapidly growing field that involves the integration of medical devices, software, and other technologies to improve patient care and outcomes. However, the increasing complexity and connectivity of IoMT systems have also led to significant security risks and challenges, which must be addressed to ensure patient privacy and data security. This research aims to develop a security model for IoMT systems that can effectively address these challenges and provide a secure and reliable framework for the deployment of IoMT solutions. The methodology outlines the procedures used to identify the security challenges and requirements of IoMT stakeholders, conduct a survey to gather data, analyze survey data, develop a security model, and validate the model in a testbed environment.

A. METHODOLOG

Various steps involved in the methodology is discussed in the following sections.

1) CONDUCT A COMPREHENSIVE LITERATURE REVIEW

The first step of the methodology is to conduct a thorough literature review to identify the security challenges and issues relevant to the Internet of Medical Things (IoMT). The literature review will include research articles, reports, and other relevant publications from various databases such as IEEE Xplore, Science Direct, ACM Digital Library, and other relevant databases. The inclusion criteria for articles will be based on keywords related to the security of IoMT, while the exclusion criteria will be based on irrelevant articles and duplicate publications.

2) IDENTIFY KEY STAKEHOLDERS AND THEIR SECURITY REQUIREMENTS

Based on the findings of the literature review, key stakeholders and their security requirements will be identified. The stakeholders may include patients, medical professionals, IT administrators, and others involved in the IoMT ecosystem. The security requirements will be categorized based on confidentiality, integrity, availability, and other relevant parameters.

3) DATA COLLECTION

Systematic Literature Review (SLR) is a rigorous and methodical approach to data collection in research that aims to minimize bias, ensure replicability, and provide a comprehensive analysis of existing literature on a specific topic. In the context of data collection, SLR involves several well-defined stages to ensure that the gathered information is accurate, reliable, and relevant to the research question. These stages include defining research questions, developing a search strategy, identifying relevant studies, applying pre-defined inclusion and exclusion criteria, and conducting a thorough quality assessment of the selected studies.

Data collection using SLR begins with the development of a protocol that outlines the scope, objectives, and methodology to be employed in the review process. The search strategy is designed to identify studies from various sources such as electronic databases, conference proceedings, and other repositories, using relevant keywords and search strings.

Once the studies are identified, researchers apply pre-defined inclusion and exclusion criteria to select relevant publications for further analysis. This step ensures that only studies of high quality and those that directly contribute to answering the research questions are included.

Following the selection of studies, researchers extract data and information related to their research questions using a standardized data extraction template. This process ensures consistency and facilitates the synthesis of findings across different studies. Finally, the collected data is synthesized, analyzed, and presented in a manner that highlights the key findings, gaps, and trends in the existing literature. By these rigorous procedures, SLR ensures a comprehensive and unbiased data collection process, enabling researchers to draw well-informed conclusions and contribute to the existing body of knowledge on a specific topic.

4) META-ANALYSIS

The data collected from the survey will be analyzed to identify the security issues and challenges faced by key stakeholders. The analysis will be conducted using various statistical tools such as descriptive statistics, regression analysis, or other relevant techniques. The results of the analysis will provide valuable insights into the security requirements and concerns of key stakeholders.

5) DEVELOP A SECURITY MODEL

Based on the findings of the literature review and survey, a security model will be developed to address the security challenges and issues identified in step 2 and step 4. The security model will be designed based on best practices, standards, and guidelines such as ISO 27001, NIST, and HIPAA. The security model will be validated by subjecting it to a thorough analysis of its ability to meet the identified security requirements.

6) VALIDATE THE SECURITY MODEL

The proposed security model will be validated by implementing it in a testbed environment. The testbed environment will simulate the IoMT architecture, solutions, and stakeholders to validate the proposed security model's effectiveness. The implementation will be conducted based on the proposed security model's guidelines.

VI. MODEL CONSTRUCTION

The primary objective of this model is to identify security risks associated with IoMT solutions, develop a access control authorization, implement security measures, and continuously improve the security framework. The inputs for this model include various stakeholders involved in IoMT, including medical professionals, device manufacturers, and I.T professionals, along with IoMT solutions such as devices, sensors, and networks, and IoMT architecture consisting of network topology, data flow, and protocols. The output of this model is a comprehensive security framework for IoMT systems that will provide effective protection against cyber threats.

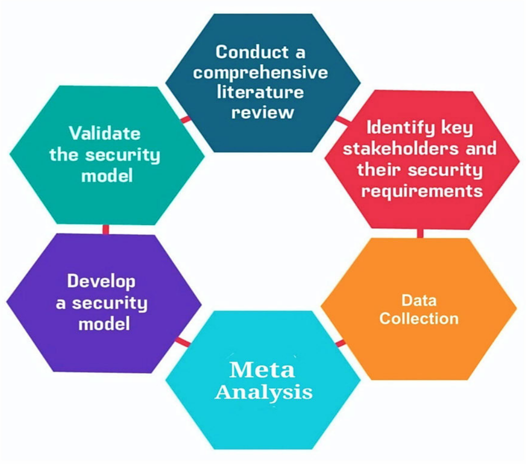

Conduct a comprehensive literature review
Identify key stakeholders and their security requirements
Data Collection
Meta Analysis
Develop a security model
Validate the security model

FIGURE 4. Stepwise methodology.

A. IoMT SECURITY FRAMEWORK: (RQ1)

i. Inputs:

- IoMT stakeholders (medical professionals, device manufacturers, IT professionals)
- IoMT solutions (devices, sensors, networks)
- IoMT architecture (network topology, data flow, protocols)

ii. Outputs:

Comprehensive security framework for IoMT systems

1. ***Identify Security Risks:***
   a. Conduct a risk assessment to identify potential security risks for the IoMT stakeholders, solutions, and architecture
   b. Identify the risks based on their likelihood and potential impact
2. ***Access Control Authorization :***
   a. Develop a security strategy that addresses the identified risks
   b. Ensure that the security strategy aligns with industry standards and best practices.
   c. Involve all stakeholders in the development of the security strategy to ensure buy-in and collaboration
3. ***Implement Security Measures:***
   a. Implement security measures to mitigate the identified risks
   b. Implement measures such as access controls, encryption, and threat detection to protect the IoMT solutions and architecture
   c. Implement policies and procedures to ensure data privacy and regulatory compliance.
4. ***Monitor and Update the Security Framework: (RQ3)***
   a. Continuously monitor the security of the IoMT solutions and architecture.

   b. Regularly update the security framework to address new and emerging threats.
   c. Conduct periodic security audits to ensure the effectiveness of the security measures.

5. ***Train and Educate Stakeholders: (RQ4)***
   a. Provide training and education to all stakeholders on the importance of security in IoMT systems
   b. Ensure that all stakeholders understand their roles and responsibilities in maintaining the security of the IoMT solutions and architecture
   c. Encourage a culture of security awareness and best practices among all stakeholders

6. ***Establish Incident Response Protocols:***
   a. Develop and implement incident response protocols to address security breaches or other incidents
   b. Ensure that all stakeholders are aware of the incident response protocols and know how to respond in the event of an incident
   c. Regularly test the incident response protocols to ensure their effectiveness.

7. ***Continuously Improve the Security Framework:***
   a. Continuously assess the effectiveness of the security framework and make improvements as necessary
   b. Stay up-to-date on new security threats and trends in the IoMT industry
   c. Ensure that the security framework evolves with the changing IoMT landscape.

The above algorithm provides a framework for developing a comprehensive security framework for IoMT stakeholders, IoMT solutions, and IoMT architecture. It emphasizes the importance of identifying and prioritizing security risks, implementing security measures, monitoring, and updating the security framework, and training and educating stakeholders.

The following is the diagram of the proposed security model for IoMT

VII. MODEL IMPLEMENTATION

The primary objective of this model is to implement the security measures identified in the model construction phase and continuously monitor and update the security framework. The implementation process includes identifying potential vulnerabilities in the IoMT system, implementing security controls, and testing the effectiveness of the implemented security measures. The inputs for this model include the comprehensive security framework developed in the model construction phase and the resources required for implementing the security measures. The output of this model is an IoMT system with a robust and effective security framework that ensures the confidentiality, integrity, and availability of patient data and prevents unauthorized access and cyber threats.

A. IoMT SECURITY MODEL INPUTS

The IoMT Security Framework is designed to be applied to IoMT stakeholders, solutions, and architecture. The inputs to the framework include:

1) IoMT STAKEHOLDERS (MEDICAL PROFESSIONALS, DEVICE MANUFACTURERS, I.T PROFESSIONALS)

The security of IoMT systems depends on the actions and decisions of various stakeholders involved in their design, development, deployment, and maintenance. This includes medical professionals who use IoMT devices to provide patient care, device manufacturers who design and build IoMT solutions, and IT professionals who manage IoMT networks and infrastructure.

2) IoMT SOLUTIONS (DEVICES, SENSORS, NETWORKS)

The security of IoMT systems also depends on the security of the devices, sensors, and networks used to collect and transmit patient data. These devices and sensors may be embedded in medical devices or worn by patients to collect vital signs and other health information, while networks may include wired and wireless connections that transmit data between devices and healthcare providers.

3) IoMT ARCHITECTURE (NETWORK TOPOLOGY, DATA FLOW, PROTOCOLS)

The security of IoMT systems also depends on the architecture and design of the overall system, including network topology, data flow, and protocols used to transmit data between devices and healthcare providers. This architecture must be designed to ensure the confidentiality, integrity, and availability of patient data, while also protecting against potential threats and vulnerabilities.

Overall, the IoMT Security Framework is designed to provide a comprehensive approach to securing IoMT systems, and the inputs to the framework must be carefully considered in order to develop an effective and comprehensive security strategy.

B. IoMT SECURITY MODEL IMPLEMENTATION HERE IS THE IMPLEMENTATION OF EACH STEP OF THE MODEL

1) IDENTIFY SECURITY RISKS

The first step in the IoMT security model is to identify security risks. This can be done using various techniques such as risk assessments, threat modeling, and vulnerability scanning.

Here is Python code to conduct a basic vulnerability scan using the nmap library:

```
import nmap
# Define target IP address and port range
target_ip = ‘192.168.0.1’
port_range = ‘1-1024’
# Create a new nmap scanner object
scanner = nmap.PortScanner()
```

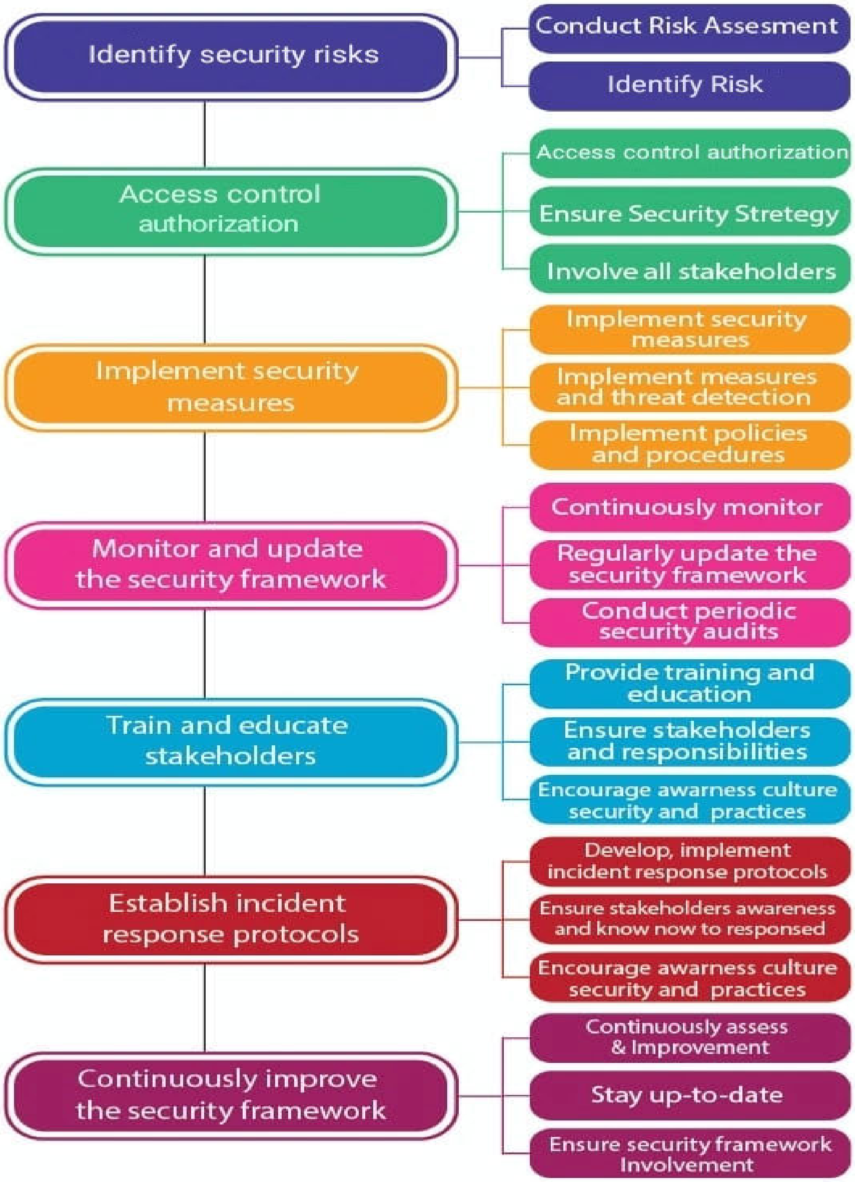

Identify security risks
Conduct Risk Assesment
Identify Risk
Access control authorization
Access control authorization
Ensure Security Stretegy
Involve all stakeholders
Implement security measures
Implement security measures
Implement measures and threat detection
Implement policies and procedures
Monitor and update the security framework
Continuously monitor
Regularly update the security framework
Conduct periodic security audits
Train and educate stakeholders
Provide training and education
Ensure stakeholders and responsibilities
Encourage awarness culture security and practices
Establish incident response protocols
Develop, implement incident response protocols
Ensure stakeholders awareness and know now to responsed
Encourage awarness culture security and practices
Continuously improve the security framework
Continuously assess & Improvement
Stay up-to-date
Ensure security framework Involvement

FIGURE 5. The security model for internet of medical things.

```
# Use nmap to scan the target for open ports
result = scanner.scan(target_ip, port_range)
# Print the results of the scan
print(result)
```

C. ACCESS CONTROL AUTHORIZATION

The next step is Access Control Authorization that addresses identified risks and aligns with industry standards and best practices. This can include developing security policies, defining security controls, and writing Python code to enforce those policies and controls.

Here is Python code to enforce a basic access control policy using Flask, a Python web framework:

```
from flask import Flask, request, abort
app Flask(_name_)
# Define a list of authorized users
authorized_users = ['Mudasir', ' Ijaz ']
# Define a Flask route that requires authentication
@app.route('/protected')
def protected_resource():
# Check if the user is authorized
if request.authorization and
```

```
request.authorization.username in
authorized_user
return “Access granted”
else:
abort(401)
# Run the Flask application
if_name_ == ’_main_’:
app.run()
```

1) IMPLEMENT SECURITY MEASURES

The third step is to implement security measures such as access control mechanisms, encryption algorithms, and threat detection mechanisms using Python code. This can involve using various Python libraries and tools such as cryptography, PyCrypto, and scapy.

Here is Python code to encrypt and decrypt data using the PyCrypto library:

```
from Crypto.Cipher import AES
import base64
Define the encryption key and initialization vector
key=“1234567890123456”
iv = ‘1234567890123456’
* Define the plaintext message to be
encrypted
plaintext = “This is a secret message
* Create a new AES cipher object and encrypt the plaintext
cipher AES.new(key, AES.MODE_CBC, iv)ciphertext =
cipher.encrypt(plaintext)
* Print the encrypted ciphertext
print(base64.b64encode(ciphertext))
∗ Create a new AES cipher object and decrypt the
ciphertext
cipher = AES.new(key, AES.MODE_CBC,
iv)decryptedtext = cipher.decrypt
(ciphertext)
# Print the decrypted plaintext
print(decryptedtext)
```

2) MONITOR AND UPDATE THE SECURITY FRAMEWORK: (RQ5)

The fourth step is to monitor and update the security framework to ensure that it remains effective and up-to-date. This can involve using Python code to log security events, conduct incident response, and update security policies and controls.

Here is Python code to log security events using the Python logging library:

```
import logging
# Create a new logging object
logger = logging.getLogger(‘security’)
# Define a file handler to log events to a file
file_handler =
logging.FileHandler(‘security.log’)
# Define a logging format
formatter = logging.Formatter(’%(asctime)s
%(name)s %(levelname)s - %(message)s
file_handler.setFormatter (formatter)
# Add the file handler to the logging object
logger.addHandler(file_handler)
# Log a security event
logger.warning(‘Unauthorized access
attempt detected’)
```

3) TRAIN AND EDUCATE STAKEHOLDERS: (RQ6)

The fifth step is to train and educate stakeholders on the importance of security in IoMT systems and best practices for maintaining security. This can involve developing training materials, conducting training sessions, and using Python code to automate security-related tasks.

Here is Python code to send email notifications to stakeholders when a security event is detected:

```
import smtplib
# Define email server and login credentials
smtp_server = ‘smtp.gmail.com’
smtp_port = 587
smtp_username = ’youremail@gmail.com
smtp_password = ‘yourpassword’
# Define a function to send email
notifications
def send_email_notification(subject, body):
message = f’Subject: (subject}\n\n{body}”
with smtplib.SMTP (smtp_server,
smtp_port) as server:
server.starttls()
server.login(smtp_username, smtp_password)
server.sendmail(smtp_username, [’user1@example.com’,
’user2@example.com’],
# Call the send_email_notification function
when a security event is detected
send_email_notification(‘Security Alert’,
‘Unauthorized access attempt detected’)
```

Here is Python code to Broadcast email notifications to stakeholders when a security event is detected:

```
import smtplib
# Define email server and login credentials
smtp_server = ‘smtp.gmail.com”
smtp_port = 587
smtp_username = ‘youremail@gmail.com’
smtp_password = ‘yourpassword’
User_list = [“admin”, “medical”, “surgery”,
“ENT”, “OT”, “ICU”, “IPD”,“OPD” ]
# Define a function to send email
notifications
def send_email_notification(subject, body):
message = f’Subject: {subject}\n\n{body}∗
with smtplib.SMTP (smtp_server,
smtp_port) as server:
server.starttls()
server.login(smtp_username, smtp_password)
server.sendmail(smtp_username, [’userslist’
]
# Call the send_email_notification function
when a security event is detected
```

```
send_email_notification(‘Security Alert’,
‘Unauthorized access attempt detected’)
```

4) ESTABLISH INCIDENT RESPONSE PROTOCOLS

The sixth step is to establish incident response protocols to ensure that all stakeholders know how to respond to potential security incidents. This can involve developing incident response plans, conducting incident response drills, and using Python code to automate incident response tasks.

Here is Python code to automatically block an IP address when a security event is detected:

```
import iptc
# Define the IP address to be blocked
ip_address 192.168.0.1’
# Define the chain and rule to block the IP
address
chain=iptc.Chain (iptc. Table
(iptc.Table.FILTER), ‘INPUT’)
rule = iptc.Rule()
rule.src = ip_address
rule.target iptc. Target (rule, ‘DROP’)
chain.insert_rule(rule)
```

D. CONTINUOUSLY IMPROVE THE SECURITY FRAMEWORK

The final step is to continuously improve the security framework by assessing its effectiveness and making improvements as necessary. This can involve conducting periodic security assessments, researching and developing new security mechanisms and controls, and using Python code to automate security-related tasks.

Beautiful soup Library (Simple techniques for exploring, finding, and altering a parse tree in HTML and XML files are provided by Beautiful Soup. It converts a complicated HTML page into a Python object tree. Also, the page is automatically converted to Unicode, so you don’t have to worry about encodings).

Here is Python code to conduct a basic security assessment:

```
import time
import subprocess
import requests
from bs4 import BeautifulSoup
#Define a function to perform periodic
security assessments using Nmap
def perfore security assessment():
target = “192.168.1.1”# Replace with your
target IP or domain
ports = “21-25,80,443” # Specify the ports
you want to scan
# Perform the scan using Nmap
scan_result =
subprocess.check_output([“map” “, ports,
target])
print(scan result.decode())
# Define a function to fetch the latest news
related to IOMT security
def fetch_font_security_news():
url=“https://example.com” # Replace with
the URL of a relevant news source
response requests.get(url)
soup = BeautifulSoup(response.content,
“htel.parser”)
headlines soup.find_all(“h2”,
class=“headline”)
for headline in headlines:
print (headline.text)
Schedule periodic tasks
assessment_interval = 60* 60* 24 # Perform
assessments every 24 hours
news_interval= 60* 60*6 #Fetch news every
6 hours
next_assessment_time = time.time()
next_news_time = time.time()
while True:
current_time time.time()
if current time > next_assessment_time:
perform_security_assessment()
next_assessment_time + =
assessment_interval
if current_time >= next_news_time:
fetch_iont_security_news()
next_news_time + news_interval
time.sleep(60) # Wait for 60 seconds before
checking again
```

VIII. CONCLUSION

In conclusion, the IoMT Security Framework developed in this research provides a comprehensive approach to addressing the security challenges facing IoMT stakeholders, solutions, and architecture. With the increasing adoption of IoMT solutions in healthcare settings, it is essential to ensure the confidentiality, integrity, and availability of patient data while also protecting against potential threats and vulnerabilities.

The IoMT Security Framework includes seven steps: identifying security risks, access authorization control, implementing security measures, monitoring and updating the security framework, training and educating stakeholders, establishing incident response protocols, and continuously improving the security framework.

By following these steps, IoMT stakeholders can develop a comprehensive and effective security strategy that addresses the specific risks and vulnerabilities facing their IoMT systems. The inputs to the framework include IoMT Stakeholders (Medical Professionals, Device Manufacturers, IT Professionals), IoMT Solutions (Devices, Sensors, Networks), and IoMT Architecture (Network Topology, Data Flow, Protocols).

Overall, the IoMT Security Framework presented in this research makes an important contribution to the field of IoMT security by providing a practical and comprehensive approach to enhancing patient data privacy and security.

However, further research is needed to develop more specific guidelines and best practices for implementing the framework in different types of IoMT systems and to address the rapidly evolving security threats facing the IoMT industry.

REFERENCES USED IN SLR

[S1] F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and privacy in the Internet of Medical Things: Taxonomy and risk assessment," in *Proc. IEEE 42nd Conf. Local Comput. Netw. Workshops*, Oct. 2017, pp. 112–120. [Online]. Available: https://ieeexplore.ieee.org/document/8110212

[S2] S. Manimurugan, S. Al-Mutairi, 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*, vol. 8, pp. 77396–77404, 2020, doi: 10.1109/ACCESS.2020.2986013.

[S3] M. Irfan and N. Ahmad, "Internet of Medical Things: Architectural model, motivational factors and impediments," in *Proc. 15th Learn. Technol. Conf. (LT)*, Feb. 2018, pp. 6–13, doi: 10.1109/lt.2018.8368495.

[S4] G. J. Joyia, R. M. Liaqat, A. Farooq, and S. Rehman, "Internet of Medical Things (IOMT): Applications, benefits and future challenges in healthcare domain," *J. Commun.*, vol. 12, pp. 240–247, Apr. 2017, doi: 10.12720/jcm.12.4.240-247.

[S5] X. Li, H.-N. Dai, Q. Wang, M. Imran, D. Li, and M. A. Imran, "Securing Internet of Medical Things with friendly-jamming schemes," *Comput. Commun.*, vol. 160, pp. 431–442, Jul. 2020, doi: 10.1016/j.comcom.2020.06.026.

[S6] K. N. Devi and R. Muthuselvi, "Parallel processing of IoT health care applications," in *Proc. 10th Int. Conf. Intell. Syst. Control (ISCO)*, Jan. 2016, pp. 1–6.

[S7] X. Huang and S. Nazir, "Evaluating security of Internet of Medical Things using the analytic network process method," *Secur. Commun. Netw.*, vol. 2020, pp. 1–14, Sep. 2020.

[S8] F. Lamonaca, E. Balestrieri, I. Tudosa, F. Picariello, D. L. Carnì, C. Scuro, F. Bonavolontà, V. Spagnuolo, G. Grimaldi, and A. Colaprico, "An overview on Internet of Medical Things in blood pressure monitoring," in *Proc. IEEE Int. Symp. Med. Meas. Appl. (MeMeA)*, Jun. 2019, pp. 1–6.

[S9] F. Alsubaei, A. Abuhussein, V. Shandilya, and S. Shiva, "IoMT-SAF: Internet of Medical Things security assessment framework," *Internet Things*, vol. 8, Dec. 2019, Art. no. 100123.

REFERENCES

[1] W. Wilkowska and M. Ziefle, "Privacy and data security in E-health: Requirements from the user's perspective," *Health Informat. J.*, vol. 18, no. 3, pp. 191–201, Sep. 2012.

[2] 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 Gener. Comput. Syst.*, vol. 98, pp. 60–68, Sep. 2019.

[3] X. Wang, L. Wang, Y. Li, and K. Gai, "Privacy-aware efficient fine-grained data access control in Internet of Medical Things based fog computing," *IEEE Access*, vol. 6, pp. 47657–47665, 2018.

[4] O. AlShorman, B. AlShorman, M. Al-khassaweneh, and F. Alkahtani, "A review of Internet of Medical Things (IoMT)—Based remote health monitoring through wearable sensors: A case study for diabetic patients," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 20, no. 1, p. 414, Oct. 2020.

[5] L. Wang, Y. Ali, S. Nazir, and M. Niazi, "ISA evaluation framework for security of Internet of Health Things system using AHP-TOPSIS methods," *IEEE Access*, vol. 8, pp. 152316–152332, 2020.

[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," *Comput. Commun.*, vol. 150, pp. 644–660, Jan. 2020, doi: 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," *Comput. Commun.*, vol. 160, pp. 111–131, Jul. 2020, doi: 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 Gener. Comput. Syst.*, vol. 98, pp. 60–68, Sep. 2019, doi: 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," *Secur. Commun. Netw.*, vol. 2020, pp. 1–14, Sep. 2020, doi: 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)," *Comput. Electr. Eng.*, vol. 72, pp. 455–467, Nov. 2018, doi: 10.1016/j.compeleceng.2018.10.009.

[11] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop, J. Rodriguez, and D. Lymberopoulos, "A survey on security threats and countermeasures in Internet of Medical Things (IoMT)," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 6, p. e4049, Jul. 2020, doi: 10.1002/ett.4049.

[12] M. Seliem and K. Elgazzar, "BIoMT: Blockchain for the Internet of Medical Things," in *Proc. IEEE Int. Black Sea Conf. Commun. Netw. (BlackSeaCom)*, Jun. 2019, pp. 1–4, doi: 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: 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 Things*, vol. 8, Dec. 2019, Art. no. 100123, doi: 10.1016/j.iot.2019.100123.

[15] O. AlShorman, B. AlShorman, M. Al-khassaweneh, and F. Alkahtani, "A review of Internet of Medical Things (IoMT)—Based remote health monitoring through wearable sensors: A case study for diabetic patients," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 20, no. 1, pp. 414–422, Oct. 2020, doi: 10.11591/ijeecs.v20.i1.pp414-422.

[16] S. Tahir, S. T. Bakhsh, M. Abulkhair, and M. O. Alassafi, "An energy-efficient fog-to-cloud Internet of Medical Things architecture," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 5, May 2019, Art. no. 155014771985197, doi: 10.1177/1550147719851977.

[17] F. Al-Turjman and B. Deebak, "Privacy-aware energy-efficient framework using the Internet of Medical Things for COVID-19," *IEEE Internet Things Mag.*, vol. 3, no. 3, pp. 64–68, Sep. 2020, doi: 10.1109/iotm.0001.2000123.

[18] M. Kumar and S. Chand, "A secure and efficient cloud-centric Internet-of-Medical-Things-enabled smart healthcare system with public verifiability," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10650–10659, Oct. 2020, doi: 10.1109/jiot.2020.3006523.

[19] Y. Sun, F. P.-W. Lo, and B. Lo, "Security and privacy for the Internet of Medical Things enabled healthcare systems: A survey," *IEEE Access*, vol. 7, pp. 183339–183355, 2019, doi: 10.1109/access.2019.2960617.

[20] C. Kotronis, I. Routis, E. Politi, M. Nikolaidou, G. Dimitrakopoulos, D. Anagnostopoulos, A. Amira, F. Bensaali, and H. Djelouat, "Evaluating Internet of Medical Things (IoMT)-based systems from a human-centric perspective," *Internet Things*, vol. 8, Dec. 2019, Art. no. 100125, doi: 10.1016/j.iot.2019.100125.

[21] V. Balasubramanian and A. Jolfaei, "A scalable framework for health-care monitoring application using the Internet of Medical Things," *Softw., Pract. Exper.*, vol. 51, no. 12, pp. 2457–2468, Jun. 2020, doi: 10.1002/spe.2849.

[22] R. Basatneh, B. Najafi, and D. G. Armstrong, "Health sensors, smart home devices, and the Internet of Medical Things: An opportunity for dramatic improvement in care for the lower extremity complications of diabetes," *J. Diabetes Sci. Technol.*, vol. 12, no. 3, pp. 577–586, Apr. 2018, doi: 10.1177/1932296818768618.

[23] E. K. Wang, C.-M. Chen, M. M. Hassan, and A. Almogren, "A deep learning based medical image segmentation technique in Internet-of-Medical-Things domain," *Future Gener. Comput. Syst.*, vol. 108, pp. 135–144, Jul. 2020, doi: 10.1016/j.future.2020.02.054.

[24] D. Nkomo and R. Brown, "Hybrid cybersecurity framework for the Internet of Medical Things (IOMT)," in *Proc. IEEE 12th Int. Conf. Global Secur., Saf. Sustainability (ICGS)*, Jan. 2019, p. 212, doi: 10.1109/icgs3.2019.8688030.

[25] D. Shin and Y. Hwang, "Integrated acceptance and sustainability evaluation of Internet of Medical Things," *Internet Res.*, vol. 27, no. 5, pp. 1227–1254, Oct. 2017, doi: 10.1108/intr-07-2016-0200.

[26] M. Elhoseny, K. Shankar, S. K. Lakshmanaprabu, A. Maseleno, and N. Arunkumar, "RETRACTED ARTICLE: Hybrid optimization with cryptography encryption for medical image security in Internet of Things," *Neural Comput. Appl.*, vol. 32, no. 15, pp. 10979–10993, Oct. 2018, doi: 10.1007/s00521-018-3801-x.

[27] D. A. Hammood, H. A. Rahim, A. Alkhayyat, and R. B. Ahmad, "Body-to-body cooperation in Internet of Medical Things: Toward energy efficiency improvement," *Future Internet*, vol. 11, no. 11, p. 239, Nov. 2019, doi: 10.3390/fi11110239.

[28] A. Limaye and T. Adegbija, "A workload characterization for the Internet of Medical Things (IoMT)," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI*, Jul. 2017, pp. 302–307. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7987536

[29] R. Kumar, A. K. Pandey, A. Baz, H. Alhakami, W. Alhakami, A. Agrawal, and R. A. Khan, "Fuzzy-based symmetrical multi-criteria decision-making procedure for evaluating the impact of harmful factors of healthcare information security," *Symmetry*, vol. 12, no. 4, p. 664, Apr. 2020, doi: 10.3390/sym12040664.

[30] K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray, and Y. Jin, "Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice," *J. Hardw. Syst. Secur.*, vol. 2, no. 2, pp. 97–110, May 2018, doi: 10.1007/s41635-017-0029-7.

[31] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure medical data transmission model for IoT-based healthcare systems," *IEEE Access*, vol. 6, pp. 20596–20608, 2018, doi: 10.1109/access.2018.2817615.

[32] M. Shen, Y. Deng, L. Zhu, X. Du, and N. Guizani, "Privacy-preserving image retrieval for medical IoT systems: A blockchain-based approach," *IEEE Netw.*, vol. 33, no. 5, pp. 27–33, Sep. 2019, doi: 10.1109/mnet.001.1800503.

[33] K. Sandya and S. Kompella, "A combined approach of steganography and cryptography with generative adversarial networks: Survey," in *Intelligent System Design: Proceedings of INDIA 2022*. Singapore: Springer, 2022, pp. 187–196.

[34] S. Pirbhulal, O. W. Samuel, W. Wu, A. K. Sangaiah, and G. Li, "A joint resource-aware and medical data security framework for wearable healthcare systems," *Future Gener. Comput. Syst.*, vol. 95, pp. 382–391, Jun. 2019, doi: 10.1016/j.future.2019.01.008.

[35] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, and A. Bouabdallah, "A systemic approach for IoT security," in *Proc. IEEE Int. Conf. Distrib. Comput. Sensor Syst.*, May 2013, pp. 351–355, doi: 10.1109/dcoss.2013.78.

[36] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, "Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives," *Cryptography*, vol. 3, no. 1, p. 3, Jan. 2019, doi: 10.3390/cryptography3010003.

[37] A. Al Hayajneh, M. Z. A. Bhuiyan, and I. McAndrew, "Improving Internet of Things (IoT) security with software-defined networking (SDN)," *Computers*, vol. 9, no. 1, p. 8, Feb. 2020, doi: 10.3390/computers9010008.

[38] J. D. Lee, T. S. Yoon, S. H. Chung, and H. S. Cha, "Service-oriented security framework for remote medical services in the Internet of Things environment," *Healthcare Informat. Res.*, vol. 21, no. 4, p. 271, 2015, doi: 10.4258/hir.2015.21.4.271.

[39] K. N. Devi and R. Muthuselvi, "Secret sharing of IoT healthcare data using cryptographic algorithm," *Int. J. Eng. Res.*, vol. 5, no. 4, pp. 790–991. 2016, doi: 10.17950/ijer/v5i4/029.

[40] E. Dellgren, "A case study on how the Apple Watch can benefit medical heart research," Bachelor Thesis, Publikationer från KTH, Digitala Vetenskapliga Arkivet-Academic Arch. On-line, Skolan för Datavetenskap och Kommunikation (CSC), KTH, Sweden, 2017.

[41] S. M. R. Islam, D. Kwak, MD. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015, doi: 10.1109/access.2015.2437951.

[42] M. Pistono, R. Bellafqira, and G. Coatrieux, "Secure processing of stream cipher encrypted data issued from IoT: Application to a connected knee prosthesis," in *Proc. 41st Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Jul. 2019, pp. 6494–6497, doi: 10.1109/embc.2019.8857055.

[43] A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun, and N. Jhanjhi, "Secure healthcare data aggregation and transmission in IoT—A survey," *IEEE Access*, vol. 9, pp. 16849–16865, 2021, doi: 10.1109/access.2021.3052850.

[44] F. Nausheen and S. H. Begum, "Healthcare IoT: Benefits, vulnerabilities and solutions," in *Proc. 2nd Int. Conf. Inventive Syst. Control*, Jan. 2018, pp. 517–522. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8399126/authors#authors

[45] S. Peng and H. Shen, "Security technology analysis of IoT," in *Internet of Things* (Communications in Computer and Information Science), vol. 312. 2012, pp. 401–408. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-32427-7_56, doi: 10.1007/978-3-642-32427-7_56.

[46] L. Fang, Y. Li, Z. Liu, C. Yin, M. Li, and Z. J. Cao, "A practical model based on anomaly detection for protecting medical IoT control services against external attacks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 6, pp. 4260–4269, Jun. 2021, doi: 10.1109/tii.2020.3011444.

[47] M. Rajasekaran, A. Yassine, M. S. Hossain, M. F. Alhamid, and M. Guizani, "Autonomous monitoring in healthcare environment: Reward-based energy charging mechanism for IoMT wireless sensing nodes," *Future Gener. Comput. Syst.*, vol. 98, pp. 565–576, Sep. 2019, doi: 10.1016/j.future.2019.01.021.

[48] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1646–1685, 3rd Quart., 2020, doi: 10.1109/comst.2020.2988293.

[49] S. Liaqat, A. Akhunzada, F. S. Shaikh, A. Giannetsos, and M. A. Jan, "SDN orchestration to combat evolving cyber threats in Internet of Medical Things (IoMT)," *Comput. Commun.*, vol. 160, pp. 697–705, Jul. 2020, doi: 10.1016/j.comcom.2020.07.006.

[50] M. A. Habib, C. M. N. Faisal, S. Sarwar, M. A. Latif, F. Aadil, M. Ahmad, R. Ashraf, and M. Maqsood, "Privacy-based medical data protection against internal security threats in heterogeneous Internet of Medical Things," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 9, Sep. 2019, Art. no. 155014771987565, doi: 10.1177/1550147719875653.

[51] R. M. P. H. K. Rathnayake, M. S. Karunarathne, N. S. Nafi, and M. A. Gregory, "Cloud enabled solution for privacy concerns in Internet of Medical Things," in *Proc. 28th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Nov. 2018, pp. 1–4, doi: 10.1109/atnac.2018.8615361.

[52] A. Strielkina, V. Kharchenko, and D. Uzun, "Availability models for healthcare IoT systems: Classification and research considering attacks on vulnerabilities," in *Proc. IEEE 9th Int. Conf. Dependable Syst., Services Technol. (DESSERT)*, May 2018, pp. 58–62, doi: 10.1109/dessert.2018.8409099.

[53] M. Banerjee, J. Lee, and K.-K.-R. Choo, "A blockchain future for Internet of Things security: A position paper," *Digit. Commun. Netw.*, vol. 4, no. 3, pp. 149–160, Aug. 2018, doi: 10.1016/j.dcan.2017.10.006.

[54] A. Gatouillat, Y. Badr, B. Massot, and E. Sejdic, "Internet of Medical Things: A review of recent contributions dealing with cyber-physical systems in medicine," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3810–3822, Oct. 2018, doi: 10.1109/jiot.2018.2849014.

[55] M. Husamuddin and M. Qayyum, "Internet of Things: A study on security and privacy threats," in *Proc. 2nd Int. Conf. Anti-Cyber Crimes (ICACC)*, Mar. 2017, pp. 93–97, doi: 10.1109/anticybercrime.2017.7905270.

[56] A. W. Atamli and A. Martin, "Threat-based security analysis for the Internet of Things," in *Proc. Int. Workshop Secure Internet Things*, Sep. 2014, pp. 35–43, doi: 10.1109/siot.2014.10.

[57] K. Habib, A. Torjusen, and W. Leister, "Security analysis of a patient monitoring system for the Internet of Things in eHealth," in *Proc. 7th Int. Conf. eHealth, Telemedicine, Social Medicine*, vol. 335, 2015, pp. 1–6.

[58] E. G. Spanakis, S. Bonomi, S. Sfakianakis, G. Santucci, S. Lenti, M. Sorella, F. D. Tanasache, A. Palleschi, C. Ciccotelli, V. Sakkalis, and S. Magalini, "Cyber-attacks and threats for healthcare—A multi-layer thread analysis," in *Proc. 42nd Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, Jul. 2020, pp. 5705–5708. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9176698

[59] J.-P.-A. Yaacoub, M. Noura, H. N. Noura, O. Salman, E. Yaacoub, R. Couturier, and A. Chehab, "Securing Internet of Medical Things systems: Limitations, issues and recommendations," *Future Gener. Comput. Syst.*, vol. 105, pp. 581–606, Apr. 2020, doi: 10.1016/j.future.2019.12.028.

[60] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, and C. Tsatsoulis, "Review of security and privacy for the Internet of Medical Things (IoMT)," in *Proc. 15th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, May 2019, pp. 457–464, doi: 10.1109/DCOSS.2019.00091.

[61] F. Giannoni, M. Mancini, and F. Marinelli, "Anomaly detection models for IoT time series data," 2018, *arXiv:1812.00890*.

[62] S. Sinche, O. Polo, D. Raposo, M. Femandes, F. Boavida, A. Rodrigues, V. Pereira, and J. Sá Silva, "Assessing redundancy models for IoT reliability," in *Proc. IEEE 19th Int. Symp. 'World Wireless, Mobile Multimedia Netw.' (WoWMoM)*, Jun. 2018, pp. 14–15, doi: 10.1109/wowmom.2018.8449816.

[63] R. M. Dijkman, B. Sprenkels, T. Peeters, and A. Janssen, "Business models for the Internet of Things," *Int. J. Inf. Manag.*, vol. 35, no. 6, pp. 672–678, Dec. 2015, doi: 10.1016/j.ijinfomgt.2015.07.008.

[64] J. Diaz-Rozo, C. Bielza, and P. Larrañaga, "Clustering of data streams with dynamic Gaussian mixture models: An IoT application in industrial processes," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3533–3547, Oct. 2018, doi: 10.1109/jiot.2018.2840129.

[65] V. Tkachenko, A. Goriushkina, and M. Kolisnyk, "Communication messaging models in IoT/WoT: Survey and application," in *Proc. Int. Sci.-Practical Conf. Problems Infocommunications. Sci. Technol.*, Oct. 2018, pp. 417–422, doi: 10.1109/infocommst.2018.8632063.

[66] C. Zheng, M. Egan, L. Clavier, G. W. Peters, and J.-M. Gorce, "Copula-based interference models for IoT wireless networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6, doi: 10.1109/icc.2019.8761783.

[67] N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Data collection and wireless communication in Internet of Things (IoT) using economic analysis and pricing models: A survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2546–2590, 4th Quart., 2016, doi: 10.1109/comst.2016.2582841.

[68] S. Y. Hashemi and F. Shams Aliee, "Dynamic and comprehensive trust model for IoT and its integration into RPL," *J. Supercomput.*, vol. 75, no. 7, pp. 3555–3584, Nov. 2018, doi: 10.1007/s11227-018-2700-3.

[69] S. Yarosh and P. Zave, "Locked or not?" in *Proc. CHI Conf. Human Factors Comput. Syst.*, May 2017, pp. 2993–2997, doi: 10.1145/3025453.3025617.

[70] C. Li, S. Li, Y. Chen, Y. T. Hou, and W. Lou, "Minimizing age of information under general models for IoT data collection," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 4, pp. 2256–2270, Oct. 2020, doi: 10.1109/tnse.2019.2952764.

[71] N. Nesa, T. Ghosh, and I. Banerjee, "Outlier detection in sensed data using statistical learning models for IoT," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2018, pp. 1–6, doi: 10.1109/wcnc.2018.8376988.

[72] J. Ju, M.-S. Kim, and J.-H. Ahn, "Prototyping business models for IoT service," *Proc. Comput. Sci.*, vol. 91, pp. 882–890, Jan. 2016, doi: 10.1016/j.procs.2016.07.106.

[73] I. Sohn, "Small-world and scale-free network models for IoT systems," *Mobile Inf. Syst.*, vol. 2017, pp. 1–9, Jan. 2017, doi: 10.1155/2017/6752048.

[74] J. Byun, S. Kim, J. Sa, S. Kim, Y.-T. Shin, and J.-B. Kim, "Smart city implementation models based on IoT technology," *Adv. Sci. Technol. Lett.*, vol. 129, no. 41, pp. 209–212, Apr. 2016, doi: 10.14257/astl.2016.129.41.

[75] R. Kolcun, D. A. Popescu, V. Safronov, P. Yadav, A. M. Mandalari, Y. Xie, R. Mortier, and H. Haddadi, "The case for retraining of ML models for IoT device identification at the edge," 2020, *arXiv:2011.08605*.

[76] B. Martinez, M. Montón, I. Vilajosana, and J. D. Prades, "The power of models: Modeling power consumption for IoT devices," *IEEE Sensors J.*, vol. 15, no. 10, pp. 5777–5789, Oct. 2015, doi: 10.1109/JSEN.2015.2445094.

[77] S. Leminen, M. Westerlund, M. Rajahonka, and R. Siuruainen, "Towards IoT ecosystems and business models," *J. Bus. Ind. Marketing*, pp. 15–26, 2012. [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/JBIM-10-2015-0206/full/html, doi: 10.1007/978-3-642-32686-8_2.

[78] M. T. Gardner, C. Beard, and D. Medhi, "Using SEIRS epidemic models for IoT botnets attacks," in in *Proc. Design Reliable Commun. Netw., 13th Int. Conf.*, 2017, pp. 1–8.

[79] S. A. Alabady, F. Al-Turjman, and S. Din, "A novel security model for cooperative virtual networks in the IoT era," *Int. J. Parallel Program.*, vol. 48, no. 2, pp. 280–295, Jul. 2018, doi: 10.1007/s10766-018-0580-z.

[80] M. Gurunathan and M. A. Mahmoud, "A review and development methodology of a LightWeight security model for IoT-based smart devices," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 2, pp. 1–10, 2020, doi: 10.14569/ijacsa.2020.0110217.

[81] A. Gabillon and E. Bruno, "A security model for IoT networks," in *International Conference on Future Data and Security Engineering, FDSE 2018: Future Data and Security Engineering*. 2018, pp. 39–56. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-03192-3_4, doi: 10.1007/978-3-030-03192-3_4.

[82] S. N. Mohanty, K. C. Ramya, S. S. Rani, D. Gupta, K. Shankar, S. K. Lakshmanaprabu, and A. Khanna, "An efficient lightweight integrated blockchain (ELIB) model for IoT security and privacy," *Future Gener. Comput. Syst.*, vol. 102, pp. 1027–1037, Jan. 2020, doi: 10.1016/j.future.2019.09.050.

[83] H. F. Atlam and G. B. Wills, "An efficient security risk estimation technique for risk-based access control model for IoT," *Internet Things*, vol. 6, Jun. 2019, Art. no. 100052, doi: 10.1016/j.iot.2019.100052.

[84] T. Varshney, N. Sharma, I. Kaushik, and B. Bhushan, "Architectural model of security threats & their countermeasures in IoT," in *Proc. Int. Conf. Comput., Commun., Intell. Syst. (ICCCIS)*, Oct. 2019, pp. 424–429, doi: 10.1109/icccis48478.2019.8974544.

[85] X. Bellekens, A. Seeam, K. Nieradzinska, C. Tachtatzis, A. Cleary, R. Atkinson, and I. Andonovic, "Cyber-physical-security model for safety-critical IoT infrastructures," in *Proc. Wireless World Res. Forum Meeting*, vol. 35, Apr. 2015, p. 18.

[86] Y.-S. Jeong, "Data storage and security model for mobile healthcare service based on IoT," *J. Digit. Converg.*, vol. 15, no. 3, pp. 187–193, Mar. 2017, doi: 10.14400/jdc.2017.15.3.187.

[87] P. Matta, B. Pant, and U. K. Tiwari, "DDITA: A naive security model for IoT resource security," in *Smart Innovations in Communication and Computational Sciences*. Jul. 2018, pp. 199–209. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-10-8971-8_19, doi: 10.1007/978-981-10-8971-8_19.

[88] M. Roopak, G. Yun Tian, and J. Chambers, "Deep learning models for cyber security in IoT networks," in *Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2019, pp. 0452–0457, doi: 10.1109/ccwc.2019.8666588.

[89] R. K. Kodali and A. Naikoti, "ECDH based security model for IoT using ESP8266," in *Proc. Int. Conf. Control, Instrum., Commun. Comput. Technol. (ICCICCT)*, Dec. 2016, pp. 629–633, doi: 10.1109/iccicct.2016.7988026.

[90] D. Li, Z. Cai, L. Deng, X. Yao, and H. H. Wang, "Retraction note: Information security model of block chain based on intrusion sensing in the IoT environment," *Cluster Comput.*, vol. 26, no. S1, p. 127, Dec. 2022, doi: 10.1007/s10586-022-03895-7.

[91] Z. Wang, X. Dong, Y. Li, L. Fang, and P. Chen, "IoT security model and performance evaluation: A blockchain approach," in *Proc. Int. Conf. Netw. Infrastructure Digit. Content*, Aug. 2018, pp. 260–264. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8525716

[92] J. Bugeja, B. Vogel, A. Jacobsson, and R. Varshney, "IoTSM: An end-to-end security model for IoT ecosystems," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2019, pp. 267–272, doi: 10.1109/percomw.2019.8730672.

[93] M. Kumar, S. Kumar, R. Budhiraja, M. K. Das, and S. Singh, "Lightweight data security model for IoT applications: A dynamic key approach," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Dec. 2016, pp. 424–428, doi: 10.1109/ithings-greencom-cpscom-smartdata.2016.100.

[94] F. Olivier, G. Carlos, and N. Florent, "New security architecture for IoT network," *Proc. Comput. Sci.*, vol. 52, pp. 1028–1033, Jan. 2015, doi: 10.1016/j.procs.2015.05.099.

[95] J.-C. Yang and B.-X. Fang, "Security model and key technologies for the Internet of Things," *J. China Universities Posts Telecommun.*, vol. 18, pp. 109–112, Dec. 2011, doi: 10.1016/s1005-8885(10)60159-8.

[96] P. Aufner, "The IoT security gap: A look down into the valley between threat models and their implementation," *Int. J. Inf. Secur.*, vol. 19, no. 1, pp. 3–14, Jun. 2019, doi: 10.1007/s10207-019-00445-y.

[97] T. Martin, D. Geneiatakis, I. Kounelis, S. Kerckhof, and I. N. Fovino, "Towards a formal IoT security model," *Symmetry*, vol. 12, no. 8, p. 1305, Aug. 2020, doi: 10.3390/sym12081305.

[98] S. Pirbhulal, W. Wu, and G. Li, "A biometric security model for wearable healthcare," in *Proc. IEEE Int. Conf. Data Mining Workshops (ICDMW)*, Nov. 2018, pp. 136–143. [Online]. Available: https://ieeexplore.ieee.org/document/8637506

[99] M. Elhoseny, A. Abdelaziz, A. S. Salama, A. M. Riad, K. Muhammad, and A. K. Sangaiah, "A hybrid model of Internet of Things and cloud computing to manage big data in health services applications," *Future Gener. Comput. Syst.*, vol. 86, pp. 1383–1394, Sep. 2018, doi: 10.1016/j.future.2018.03.005.

[100] R. M. S. Priya, P. K. R. Maddikunta, M. Parimala, S. Koppu, T. R. Gadekallu, C. L. Chowdhary, and M. Alazab, "An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture," *Comput. Commun.*, vol. 160, pp. 139–149, Jul. 2020, doi: 10.1016/j.comcom.2020.05.048.

[101] P. Kumar, G. P. Gupta, and R. Tripathi, "An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks," *Comput. Commun.*, vol. 166, pp. 110–124, Jan. 2021, doi: 10.1016/j.comcom.2020.12.003.

[102] D. Rizk, R. Rizk, and S. Hsu, ''Applied layered-security model to IoMT,'' in *Proc. IEEE Int. Conf. Intell. Secur. Inform.*, Jul. 2019, p. 227. [Online]. Available: https://ieeexplore.ieee.org/document/8823430.

[103] M. Tawalbeh, M. Quwaider, and L. A. Tawalbeh, ''Authorization model for IoT healthcare systems: Case study,'' in *Proc. 11th Int. Conf. Inf. Commun. Syst.*, Apr. 2020, pp. 337–342. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9078998

[104] S. Abbas and A. M. Mahmoud, ''DiaMe: IoMT deep predictive model based on threshold aware region growing technique,'' *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 11, no. 5, p. 4250, Oct. 2021, doi: 10.11591/ijece.v11i5.pp4250-4262.

[105] H. Turabieh, A. A. Salem, and N. Abu-El-Rub, ''Dynamic L-RNN recovery of missing data in IoMT applications,'' *Future Gener. Comput. Syst.*, vol. 89, pp. 575–583, Dec. 2018, doi: 10.1016/j.future.2018.07.006.

[106] A. H. M. Aman, W. H. Hassan, S. Sameen, Z. S. Attarbashi, M. Alizadeh, and L. A. Latiff, ''IoMT amid COVID-19 pandemic: Application, architecture, technology, and security,'' *J. Netw. Comput. Appl.*, vol. 174, Jan. 2021, Art. no. 102886, doi: 10.1016/j.jnca.2020.102886.

[107] S. Rani, S. H. Ahmed, R. Talwar, J. Malhotra, and H. Song, ''IoMT: A reliable cross layer protocol for Internet of multimedia things,'' *IEEE Internet Things J.*, vol. 4, no. 3, pp. 832–839, Jun. 2017, doi: 10.1109/jiot.2017.2671460.

[108] M. Sikarndar, W. Anwar, A. Almogren, I. Ud Din, and N. Guizani, ''IoMT-based association rule mining for the prediction of human protein complexes,'' *IEEE Access*, vol. 8, pp. 6226–6237, 2020, doi: 10.1109/access.2019.2963797.

[109] E. A. Adeniyi, R. O. Ogundokun, and J. B. Awotunde, ''IoMT-based wearable body sensors network healthcare monitoring system,'' in *IoT in Healthcare and Ambient Assisted Living*. 2021, pp. 103–121. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-15-9897-5_6, doi: 10.1007/978-981-15-9897-5_6.

[110] H. Abie and I. Balasingham, ''Risk-based adaptive security for smart IoT in eHealth,'' in *Proc. 7th Int. Conf. Body Area Netw.*, 2012, pp. 269–275, doi: 10.4108/icst.bodynets.2012.250235.

[111] A. M. Joshi, P. Jain, and S. P. Mohanty, ''Secure-iGLU: A secure device for noninvasive glucose measurement and automatic insulin delivery in IoMT framework,'' in *Proc. IEEE Comput. Society Annu. Symp.*, Jul. 2020, pp. 440–445. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9155014.

[112] A. Palve and H. Patel, ''Towards securing real time data in IoMT environment,'' in *Proc. 8th Int. Conf. Commun. Syst. Netw. Technol.*, Nov. 2018, pp. 113–119. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8820213/

[113] I. Benbasat, A. Bruckman, J. Carey, S. Djamasbi, U. Farooq, D. Gefen, M. Germonprez, K. Hassanein, M. Head, T. Hess, and S. Y. Ho, ''Transactions on human-computer interaction,'' *AIS Trans. Hum.-Comput. Interact.*, vol. 3, no. 1, pp. 1–25, 2011. [Online]. Available: https://aisel.aisnet.org/thci/vol1/iss4/2

[114] B. Cao, X. Wang, W. Zhang, H. Song, and Z. Lv, ''A many-objective optimization model of industrial Internet of Things based on private blockchain,'' *IEEE Netw.*, vol. 34, no. 5, pp. 78–83, Sep. 2020, doi: 10.1109/mnet.011.1900536.

[115] H. Al-Aqrabi, A. P. Johnson, R. Hill, P. Lane, and L. Liu, ''A multi-layer security model for 5G-enabled industrial Internet of Things,'' in *Proc. Int. Conf. Smart City Informatization*, Singapore: Springer, 2019, pp. 279–292, doi: 10.1007/978-981-15-1301-5_23.

[116] X. Yang, Z. Li, Z. Geng, and H. Zhang, ''A multi-layer security model for Internet of Things,'' in *Internet of Things*. 2012, pp. 388–393. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-32427-7_54, doi: 10.1007/978-3-642-32427-7_54.

[117] J. Liu, M. Chen, and L. Wang, ''A new model of industrial Internet of Things with security mechanism—An application in complex workshop of diesel engine,'' *Proc. Inst. Mech. Eng., C, J. Mech. Eng. Sci.*, vol. 234, no. 2, pp. 564–574, Jan. 2020, doi: 10.1177/0954406219884970.

[118] H. Hui, C. Zhou, S. Xu, and F. Lin, ''A novel secure data transmission scheme in industrial Internet of Things,'' *China Commun.*, vol. 17, no. 1, pp. 73–88, Jan. 2020, doi: 10.23919/jcc.2020.01.006.

[119] W. Liang, M. Tang, J. Long, X. Peng, J. Xu, and K.-C. Li, ''A secure FaBric blockchain-based data transmission technique for industrial Internet-of-Things,'' *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3582–3592, Jun. 2019, doi: 10.1109/tii.2019.2907092.

[120] D. He, M. Ma, S. Zeadally, N. Kumar, and K. Liang, ''Certificateless public key authenticated encryption with keyword search for industrial Internet of Things,'' *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3618–3627, Aug. 2018, doi: 10.1109/tii.2017.2771382.

[121] Q. Zhang, Y. Li, R. Wang, L. Liu, Y. Tan, and J. Hu, ''Data security sharing model based on privacy protection for blockchain-enabled industrial Internet of Things,'' *Int. J. Intell. Syst.*, vol. 36, no. 1, pp. 94–111, Oct. 2020, doi: 10.1002/int.22293.

[122] Z. Yang, J. He, Y. Tian, and J. Zhou, ''Faster authenticated key agreement with perfect forward secrecy for industrial Internet-of-Things,'' *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6584–6596, Oct. 2020, doi: 10.1109/tii.2019.2963328.

[123] Y. Miao, X. Liu, R. H. Deng, H. Wu, H. Li, J. Li, and D. Wu, ''Hybrid keyword-field search with efficient key management for industrial Internet of Things,'' *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3206–3217, Jun. 2019, doi: 10.1109/tii.2018.2877146.

[124] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, ''Internet of Things security: A survey,'' *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, Jun. 2017, doi: 10.1016/j.jnca.2017.04.002.

[125] H. Naeem, F. Ullah, M. R. Naeem, S. Khalid, D. Vasan, S. Jabbar, and S. Saeed, ''Malware detection in industrial Internet of Things based on hybrid image visualization and deep learning model,'' *Ad Hoc Netw.*, vol. 105, Aug. 2020, Art. no. 102154, doi: 10.1016/j.adhoc.2020.102154.

[126] E. Vasilomanolakis, J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier, and P. Kikiras, ''On the security and privacy of Internet of Things architectures and systems,'' in *Proc. Int. Workshop Secure Internet Things (SIoT)*, Sep. 2015, pp. 49–57, doi: 10.1109/siot.2015.9.

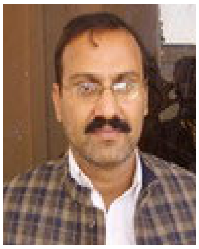
[127] J. M. Mcginthy and A. J. Michaels, ''Secure industrial Internet of Things critical infrastructure node design,'' *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8021–8037, Oct. 2019, doi: 10.1109/jiot.2019.2903242.

[128] N. Gulati and P. D. Kaur, ''Towards socially enabled Internet of Industrial Things: Architecture, semantic model and relationship management,'' *Ad Hoc Netw.*, vol. 91, Aug. 2019, Art. no. 101869, doi: 10.1016/j.adhoc.2019.101869.

[129] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, ''Systematic literature reviews in software engineering—A systematic literature review,'' *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, Jan. 2009, doi: 10.1016/j.infsof.2008.09.009.

MUDASIR MAHMOOD received the bachelor's degree in computer science from Gomal University, Dera Ismail Khan, Pakistan, in 2007. He is currently pursuing the Ph.D. degree in computer science. He is an Additional Director of the IT Quaid-e-Azam Campus, Gomal University. He is the author of several international publications. His research interests include software engineering, the Internet of Things, the Internet of Medical Things, deep learning, ands machine learning.

MUHAMMAD IJAZ KHAN is currently the Director of IT with the Institute of Computing and Information Technology, Gomal University, Dera Ismail Khan. He is an active researcher. He is the author of several international publications. His research interests include requirement engineering, software engineering, and agile methods.



ZIAUDDIN received the Diploma degree in computer forensics from the School of Education, Indiana University, USA, and the M.Sc. degree in computer science from Peshawar University. He was an Assistant Professor with the COMSATS Institute of Information Technology, Vehari. He was with Gomal University, Dera Ismail Khan, for 22 years. He is currently the Director of ICIT with Gomal University. He has published more than 18 research articles in reputed international journals. His research interests include software engineering, software process improvement, software reliability engineering, software development improvement, software quality assurance, and requirement engineering. He received the Gold Medalist from Peshawar University for the M.Sc. degree in computer science.

HAMEED HUSSAIN received the bachelor's degree in information technology from Gomal University, Dera Ismail Khan, Pakistan, in 2007, and the M.S. and Ph.D. degrees in computer science from the COMSATS Institute of Information Technology (CIIT), Pakistan, in 2009 and 2017, respectively. He is an active researcher. He is the author of several international publications. His research interests include optimization, machine learning, fog and edge computing, the Internet of Things, real-time systems, resource allocation, and load balancing in high-performance computing.

INAYAT KHAN received the Ph.D. degree in computer science from the Department of Computer Science, University of Peshawar, Pakistan. He is currently an Assistant Professor of computer science with the University of Engineering and Technology, Mardan, Pakistan. His current research is based on the design and development of context-aware adaptive user interfaces for minimizing drivers' distractions. His research interests include lifelogging, healthcare, deep learning, ubiquitous computing, accessibility, and mobile-based assistive systems for people with disabilities.

SHAHID RAHMAN received the bachelor's degree in mathematics, physics, and computer science from the University of Swat, Khyber Pakhtunkhwa, Pakistan, the M.Sc. degree in computer science from Islamia College University, Peshawar, and the M.S. degree in computer science from The University of Agriculture, Peshawar (AUP). He is currently pursuing the Ph.D. degree in computer science with the Qurtuba University of Science and Technology, Peshawar. He has over eight years of experience in academia and research. He is a Lecturer with the Department of Computer Science, University of Buner, Khyber Pakhtunkhwa. He has published several research papers in leading journals and conferences. His current research interests include software engineering, cryptography, steganalysis and steganography, computer vision, machine learning, and deep learning.

MUHAMMAD SHABIR received the M.S.C.S. degree in computer science from Islamia College University, Peshawar, Pakistan, in 2015, where he is currently pursuing the Ph.D. degree with the Department of Computer Science. He is a Lecturer with the University of Buner. His research interests include artificial intelligence, machine learning, deep learning, computer vision, and natural language processing.

BADAM NIAZI received the M.S. degree from the Department of Computer Science, University of Peshawar. He is currently an Assistant Professor of computer science with the Faculty of Computing, Nangarhar University, Jalalabad, Pakistan. He has published several research papers in well reputed international journals and conferences. His research interest includes mobile-based assistive technologies for the special with special needs.