Journal of Multidisciplinary Healthcare

Dovepress
open access to scientific and medical research

Open Access Full Text Article

REVIEW

Internet of Medical Things Security Frameworks for Risk Assessment and Management: A Scoping Review

Katerina Svandova*, Zdenek Smutny*

Faculty of Informatics and Statistics, Prague University of Economics and Business, Prague, Czech Republic

*These authors contributed equally to this work

Correspondence: Zdenek Smutny, Faculty of Informatics and Statistics, Prague University of Economics and Business, W. Churchill Sq. 1938/4, 130 67 Prague 3, Prague, Czech Republic, Email zdenek.smutny@vse.cz

Background: The massive expansion of the Internet of medical things (IoMT) technology brings many opportunities for improving healthcare. At the same time, their use increases security risks, brings security and privacy concerns, and threatens the functioning of healthcare facilities or healthcare provision.

Purpose: This scoping review aims to identify progress in designing risk assessment and management frameworks for IoMT security. The frameworks found are divided into two groups according to whether frameworks address the technological design of risk management or assess technological measures to ensure the security of the IoMT environment. Furthermore, the article intends to find out whether frameworks also include an assessment of organisational measures related to IoMT security.

Methods: This review was prepared using PRISMA ScR guidelines. Relevant studies were searched in the citation databases Web of Science and Scopus. The search was limited to articles published in English between 2018 and 17 September 2023. The initial search yielded 1341 articles, of which 44 (3.3%) were included in the scoping review. A qualitative content analysis focused on selected security perspectives and progress in the given area was carried out.

Results: Thirty-two articles describe the design of risk assessment and management frameworks. Twelve articles describe the design of frameworks for assessing the security of IoMT devices and possibly offer a comparison of different IoMT alternatives. A description of the included articles was prepared from the selected security perspectives.

Conclusion: The review shows the need to create comprehensive or holistic frameworks for operational security and privacy risk management at all layers of the IoMT architecture. It includes the design of specific technological solutions and frameworks for continuously assessing the overall level of information security and privacy of the IoMT environment. Unfortunately, none of the found frameworks offer an assessment of organizational measures even though the importance of the organization measures was highlighted in articles. Another area of interest for researchers could be the design of a general risk management database for IoMT, which would include potential IoMT-related risks connected to a particular device.

Keywords: cybersecurity, healthcare, information systems, IoMT, internet of things, IoT, threat, sensors

Introduction

Medical devices, equipment, sensors and applications that use wireless networks and the Internet to connect are referred to as the Internet of medical things (IoMT),[1] formerly also referred to as the medical Internet of things.[2] Their rapid spread in recent years has enabled the collection of patient health data, patient monitoring, automation of certain processes and subsequent analysis of the data collected. Examples include smart watches and wristbands, sensor-equipped medical devices such as glucose meters, electrocardiogram devices, blood pressure monitors, as well as sensors that monitor patients remotely, enabling monitoring of the patient's vital signs, and possibly also detecting falls. Healthcare systems face increasing numbers of patients and associated challenges.[3] The use of IoMT has the potential to make diagnosis more accurate, enable earlier detection of disease, improve patients' quality of life and reduce

Received: 16 January 2024
Accepted: 21 April 2024
Published: 13 May 2024

healthcare costs. It also means increasing the ability to incorporate advanced technologies, such as artificial intelligence, to support correct diagnosis.[4]

The IoMT is a subset of devices connected to the environment via the Internet, the so-called Internet of things (IoT). Typically, these devices have sensors, low power consumption, small memory capacity and data processing capability. Data and services are provided to users remotely.[5] This is a diverse technology found in healthcare facilities that share a common way of connecting to the outside world via the Internet. This poses an increased security risk. At the same time, their use and operation involve collecting and sharing sensitive data about individual patients. A potential cyberattack threatens not only the specific device and its functioning but also, due to the connection to other hospital systems, endangering the health and life of patients.

Karie et al[6] provide an overview of discussed security and privacy concerns.

Security concerns:

- data and information leakage,
- eavesdropping,
- hacking,
- software exploitation,
- IoT device security,
- IoT device hijacking and ransomware,
- technology-minded and security-aware users,
- insufficient IoT device testing and updates,
- lack of active device monitoring,
- shortage of efficient and robust security protocols,
- impersonation,
- health and safety of users,
- denial of service (DoS/DDoS),
- other security threats (eg, password theft, corruption, weak passwords, etc.).

Privacy concerns:

- data storage and usage,
- tracking and location privacy,
- context-aware or situational privacy,
- sensed, generated or collected data privacy,
- user privacy information mining,
- other privacy concerns (eg, dependency on device manufacturers, transparency, data collection without user consent, etc.).

Mentioned security and privacy concerns include all stakeholders (patients, medical staff, information managers, management of health facilities, equipment manufacturers) who are related to the operation of IoMT. Unfortunately, as is stated in subsections Contemporary review articles and Rationale, no review article was found addressing progress in security frameworks for assessing and managing risks for the IoMT and security frameworks for assessing the information system security level using IoMT in healthcare. Therefore, it is appropriate to carry out a scoping review first, which focuses mainly on identifying knowledge gaps, the scope and the body of articles.[7] A scoping review should be a precursor to a detailed and deeper review.

From the point of view of the scoping review focus, it is necessary to address solutions (eg, frameworks, models) designed specifically for the IoMT or more general IoT solutions designed for healthcare, among others, in the context of security risk assessment and management, and assessing the information system security level. This article goes in this direction.

The expected main contributions of this scoping review are two. The first is a scientific contribution to building a theoretical base in the area of IoMT with an emphasis on the sociotechnical perspective, which deals in particular with security risk assessment and management, and assessing the information system security level in healthcare facilities.

This area is currently not well theoretically mapped. The second is a practical benefit for professionals, offering a synthesized overview of the various solutions that have been developed in the last 5 years.

In the remainder of the section, to better understand the research activities in the field, a search of contemporary review articles was performed in subsection Contemporary review articles. Subsequently, the need to carry out this scoping review can be justified in detail in the context of what is already known from existing review articles, see subsection Rationale. At the end of this section, it can be the objectives set, see subsection Objectives.

Contemporary Review Articles

In the Web of Science (WoS) and Scopus databases, the authors searched for review articles dealing with Io(M)T security [keywords: review and security and framework and (IoT or "Internet of Things"); review and security and framework and IoMT]. None of the reviews deals with issues connected with IoMT security frameworks for risk assessment and management. In the following three subsections, the most relevant review articles focusing on the security and privacy of the Io(M)T published between 2018 and 2023 are selected from the authors' perspective. Thematically, review articles can be divided into three areas, each area being structured from general IoT basics to specific IoMT approaches:

1. The first area deals with the identification of security issues and risks associated with the Io(M)T environment and proposals for addressing them.
2. The second area assesses the applicability of current conventional security standards and assessment frameworks to Io(M)T environments.
3. The third area includes other reviews that focus on a specific domain, eg, a review of publications on the use of a particular technology or an assessment of the architectures in use.

Identification of Security Issues and Risks Associated with the Io(M)T Environment

A review[5] focused on IoT security in general categorises security risks and state-of-the-art solutions. Blockchain as the only solution is given its own chapter. The authors point out the vulnerability of blockchain caused by the limited randomness of private keys of blockchain accounts. A systematic review[8] describes current security, privacy and trust trends in IoMT-enabled smart healthcare systems, such as the use of blockchain, authentication and authorization techniques or privacy-preserving approaches. It highlights the need for developing lightweight intrusion detection systems for IoMT. An overview of the current major solutions in the field of security and privacy is also described in the review,[9] highlighting circular economy issues in IoMT. After describing security threats, a comprehensive review[10] presents a comparative analysis of existing security protocols in IoMT environments. These are the authentication, access control, intrusion detection, and key management protocols.

In 2019, a paper[11] was published describing over a hundred networked medical devices and their vulnerabilities. These are different types of IoMT, such as wearable devices, implantable devices, on-site hospital equipment and apps tracking physiological information. Vulnerabilities from a security perspective are intertwined with privacy concerns, as some security threats can affect safety and patient privacy. The authors analyse current solutions and describe research areas that must be addressed to secure networked medical devices and divide the described areas of future directions into three parts. The first deals with security mechanisms for on-site legacy medical devices, for which the topics include self-authentication, encryption, and access control mechanisms. The next subsection is about security mechanisms for implantable and wearable medical devices, describing trust management, standardized key-management techniques, lightweight cryptographic protocols and authentication mechanisms and firmware modification prevention schemes. The third area is communication technologies, where the authors point out the need to focus research on Bluetooth low energy security mechanisms and radio channel interference. Only the issues of current privacy solutions in the smart healthcare environment are addressed in the systematic review.[12] It discusses in detail the differences between the terms "security" and "privacy". Security refers to the prevention of unauthorised access, breach, modification, destruction or disclosure of data, whereas privacy refers to the storage, use and disclosure of user data according to the preferences of the data owner. Privacy ensures a person's right to make decisions about information disclosure, retention and deletion. In the case of

smart health systems, the data owner is the patient. Techniques that ensure privacy include access control, cryptography, anonymization and blockchain. A review[13] presents IoMT applications, standard protocols, security and privacy issues, and market opportunities. The paper's primary focus is the IoMT environment, emphasising protocols, architectures and platforms. The last review[14] discusses the IoMT environment, specifically the security challenges related to IoT cloud, ie, the area of integrating the IoT with cloud computing. It describes both the security issues and their solutions.

Security Standards and Assessment Frameworks for Io(M)T

Khan and Salah[5] describe existing security standards and assessment frameworks in relation to IoT-based smart environments. Although conventional security standards and assessment frameworks are not directly targeted in IoT environments, the authors believe they can be adapted for this domain. The findings highlight the lack of security standards and assessment frameworks for the IoT domain. A problematic factor typical of IoT environments is installations and configurations performed by users who are not IT experts.

The study[15] provides an overview and analysis of existing risk assessment methods and management standards. It divides the analysed existing standards and frameworks into three categories: trust-risk awareness methods, models and standards; trust-risk awareness in IoT, IoMT and e-health; and trust-risk awareness in access control. Based on an evaluation of their suitability in relation to the specifics of the IoMT, the authors conclude that their use does not sufficiently cover the risks associated with the IoMT environment. Therefore, the authors present their proposal for a security risk management approach within e-health systems.

Also, another work[16] performs an analysis of popular cybersecurity frameworks. Here, too, the authors state that they cannot cover new security risks related to IoT specifics. The authors propose a new method for risk score computing for IoT, enabling the classification and quantification of IoT risks to determine the risk level of individual IoT devices, especially in the IoMT.

Other Overview Articles and Conclusion

The main focus of the review[17] is trust-based security frameworks. According to the authors, creating a general trust framework is difficult due to the nature of the concept of trust and the fact that values can vary over a small range of many factors. Sultan et al[18] describe the security issues covered by using blockchain based on existing solutions found in the literature: data integrity, data privacy, trusted data origin, removing third-party risks, access control, illegal use of personal data, single points of failure, and scalability. The paper also highlights a risk that is not prevented by the implementation of blockchain, which is user anonymity, where a user can be found using a combination of the public key and IP address used.

Zhou et al[19] focused on IoT in general and created seven categories of IoT-specific vulnerabilities, in which the authors included twenty logic bugs and one weakness. The authors also assigned a corresponding common weakness enumeration number to these bugs.

A systematic review[20] evaluates each type of architecture, starting from the first published architecture in 2008, in terms of its emphasis on addressing security and data privacy concerns. Security is more concerned with data protection, whereas data privacy focuses on the right of individuals to control their personal data and determine what data can be shared. Among other things, the paper concludes that the included IoT architectures do not consider privacy concerns. This becomes a critical factor for the further diffusion and use of the IoT. Addressing security and privacy must be an integral part of the architectural design.

Rationale

The area of IoMT security and privacy is rapidly developing, mainly due to the significant impact on patients' health and life and the massive increase in the number of Io(M)T devices. Many published papers on IoMT security, see subsection Contemporary review articles, have previously outlined areas of research to focus on, such as self-authentication mechanisms, encryption techniques, trust management for implantable and wearable medical devices, lightweight cryptographic protocols, authentication mechanisms, and radio channel interference. These articles also marginally mention the specifics of the IoMT field due to the high number of stakeholders with a lack of information security awareness.

Yet, no review article addressing sociotechnical aspects was found to ascertain whether there are frameworks aimed at addressing this issue. The reviews published to date dealing with security assessment frameworks described in subsection

Security standards and assessment frameworks for Io(M)T evaluate existing popular approaches (eg, OCTAVE, NIST) for ensuring security and their suitability for the IoMT domain.

However, it is unclear what progress has been made in designing security frameworks for assessing and managing risks for the IoMT and with what proposed technology solutions. Related to this is the progress in the design of security frameworks for assessing the information system security level in healthcare facilities in conjunction with the use of the IoMT. For these reasons, this scoping review was prepared to systematically map the research done in this area and identify existing gaps in knowledge and possible future research directions.

Objectives

This review aims to identify risk assessment and management frameworks for IoMT security published in 2018–2023 and to see what the proposed solutions include. For the frameworks found, it is determined whether frameworks address technology design for risk assessment and management or technology assessment measures to determine the level of security of the IoMT environment, both current and for the purpose of future selection of suitable devices. It is also investigated whether frameworks include an assessment of organisational measures related to IoMT security.

The selected time period is related to the increasing complexity of cyberattacks on hospital facilities and their increasing frequency. One of the most significant events that has affected the threat perception of cyberattacks is the WannaCry ransomware attack that affected many organizations on several continents in May 2017. This attack had a particularly severe impact on the healthcare sector in England, where the healthcare facilities were locked out of their information systems, access to medical records and the use of medical devices. Dozens of National Health Service hospitals were affected, providing acute care, specialist medical services, etc. Within a week of this attack, activity at the affected facilities was reduced. The value of this reduction has been quantified at £5.9m.[21] According to a 2017 study,[22] 64% of all German hospitals were affected by a cyberattack. This trend has triggered a response from researchers who have begun to focus on securing the healthcare sector, including securing vulnerable medical devices.[22] In the same year, a hospital in New York[23] was attacked, and estimates talk about nearly $10 million for hardware recovery, software, extra staff hours, and economy loss. Subsequent repairs and security upgrades to the hospital's information system are calculated at $250,000 to $450,000. The study[23] highlights equipment such as infusion pumps, ventilators, and others that hackers can use as an entry point into the information system if not sufficiently secured. Due to the sharp increase in attacks on hospital facilities in 2017 and the increasing number of articles in WoS and Scopus in recent years, the authors focused on studies published after 2018.

As pointed out in subsection Contemporary review articles, the specific of IoMT is a high number of stakeholders with a lack of information security awareness. These are, in particular, medical staff whose primary focus is patient care. Authors of the paper[24] presented "Education and policies" as one part of security assessment. This includes healthcare professionals and patients who become part of the environment by using IoMT devices and need to be sufficiently trained. The paper[23] also cites limited training for staff on safe cyber practices as one of the problems with increasing cyberattacks. These points can be seen as sociotechnical aspects in the context of IoMT security, where interaction between users and the information system directly or through the use of IoMT devices occurs. Activities aimed at educating users in terms of the safe use of technology include raising awareness of security in the Internet environment, in the internal hospital system environment, possibly internal rules for the use of bring your own device (BYOD), the importance of keeping the applications used in an updated form, training on cyberattacks, their types, possible consequences, etc.

Based on the above, the following research questions (RQ) were defined:

RQ 1 – *What progress has been made in designing security frameworks for assessing and managing risks for the IoMT and with what proposed technology solutions?*

This question aims to find security frameworks proposing specific technology solutions to enable security risk assessment and management. The output may be useful for system administrators of healthcare facilities who need to adapt information system security assurance to this trend due to the rapid proliferation of IoMT use.

RQ 2 – *What progress has been made in developing security frameworks for assessing the level of information system security in healthcare facilities (hospitals) in conjunction with the use of the IoMT? Do these frameworks include an assessment of organisational measures?*

The aim of the question is to find out whether healthcare facilities already have a tool to help identify information system vulnerabilities with respect to IoMT specificities, not only technological but also sociotechnical. The output presents the current options for the stakeholders involved in information system security. These are mainly IT specialists, but possibly also health technology specialists, clinical innovation specialists and others.

Methods

This review has been prepared using the PRISMA ScR (Preferred Reporting Items for Systematic Reviews and Meta-Analyses Extension for Scoping Reviews) checklist;[25] see Appendix 1. This scoping review did not require ethics or institutional review board approval, as data were collected by reviewing published peer-reviewed articles.

Literature Search

The search was conducted in the international citation indexes WoS and Scopus between January and September 2023. The last search was conducted on 17 September 2023. To search for articles, combinations of the words IoMT, IoT, healthcare, security, framework, risk, and assessment were used in the article's title or abstract; see Appendix 2. A filter was used to limit the time period to 2018–2023. Only papers available in English were included.

Selection Process

The retrieved articles were registered in the citation tool Zotero, which was used to remove duplicate records. Screening was conducted in the systematic review software Rayyan[26] by examining the abstract in terms of inclusion criteria in Table 1 and defined RQ. Both authors (K.S. and Z.S.) selected articles that met inclusion criteria in mutual cooperation. The full text was used where it was impossible to decide on inclusion or exclusion based on the abstract. Inclusion in the review was verified by examining the full text. Articles were included in this scoping review if the authors stated that their paper assesses and manages the risks arising from the involvement and use of the IoMT in an information system or addresses the security assessment of an information system using the IoMT.

Charting the Data

Data from the included papers were collected based on the examination of the full texts. For this purpose, a content analysis was carried out in accordance with the general focus of scoping reviews.[7] An instrument (form) was prepared to collect information about included articles and IoMT security frameworks, see Appendix 3.

The following information was involved: title of the work, authors, year of publication, country (first author's country of origin), article assigned to which RQ, details of the focus of the designed solution (determining whether it is framework for risk assessment and management, limitation to a specific threat, privacy concern, determining whether

Table 1 Inclusion and Exclusion Criteria

Criterion	Inclusion	Exclusion
Abbreviation IoMT	Internet of medical things	Different meaning
Type of paper	Research paper or conference paper	Any type of review, conference abstract
Period	1 January 2018 to 17 September 2023	Before 1 January 2018 and after 17 September 2023
Language	English	All other languages
Research topic	Security frameworks for risk assessment and management for IoMT environment	Security frameworks for risk assessment and management for other environments than IoMT
Research topic	Security frameworks for risk assessment and management for IoT environment in healthcare	Security frameworks for risk assessment and management for other environments than IoT in healthcare
Multiple versions	Latest version	Previous versions

it is framework for assessing the security level, assessment of the current IoMT environment, evaluation of possible IoMT acquisition alternatives, assessment of organisational measures), evaluation of the solution, limitations, future work. The information from the filled out form was used to synthesise information from the included articles qualitatively. The full text of the articles was used if more detailed information was needed. Based on the study of the described frameworks, the works were divided thematically into two groups to answer the RQs.

Results

Study Selection

The WoS and Scopus databases search based on the selected word combinations revealed 1341 papers. After removing duplicate records, 759 studies were included in the abstract screening and relevance assessment. A total of 710 papers were excluded for various reasons: 608 papers were not risk assessment papers, 46 papers did not match the required publication type, in 52 cases the abbreviation IoMT did not stand for Internet of medical things, 3 articles were not published in English, 3 frameworks were focused on IoMT developers, and 1 paper presented a method for developing a security framework.

As a result, 49 papers were identified, and then the full text was examined for inclusion in the review. Two papers were excluded due to the unavailability of the full text, and three works were excluded because these works were older versions of the included frameworks. The final number of included studies is 44, as mentioned in Figure 1.

Study Characteristics

A total of 44 papers were included in the review. These are articles from scientific journals (n=26) and conference papers (n=18). The frameworks focus either directly on the IoMT and the healthcare sector or propose frameworks for the IoT in general, with an outline of possible applications in healthcare.[16] Upon examination of the full text, it was found that two papers by the same collective of authors[15,27] describe essentially the same framework. Both papers were included in the review because the authors in[15] describe the design of a risk management system falling under RQ 1, whereas paper[27] states that it is not only a method to enable operational risk management (falling under RQ 1), but also a risk assessment to help select the most suitable medical device from different alternatives, which falls under RQ 2. The risk calculation is described similarly, but the paper[27] additionally presents a method to calculate the risk probability, including examples of weights. The papers do not refer to each other. Both papers refer in the references to different conference papers by authors of the same title from 2020. The frameworks included in the review are presented in Appendix 3.

Description of Included Studies

Advances in Security Frameworks for Risk Assessment and Management for IoMT

Thirty-two papers describing proposed frameworks for operational risk management were included in the review in relation to RQ 1. The framework's focus is limited to a specific threat type, see Appendix 3, column 1.1, or the authors do not specify a limitation to a particular threat type. Most frameworks are focused on Intrusion detection (n=8), False data injection (n=3) and Malware detection (n=3). Eight works do not specify a limitation to a particular threat type; the rest have individual focuses. Seven papers explicitly mention that their solutions also address privacy concerns. Twenty-two works use machine learning (ML), extreme learning machine (ELM) or deep learning. Five frameworks do not indicate whether an evaluation has been carried out. For other frameworks, information on verification is provided in Appendix 3. The distribution by publication time and threat type focus is shown in Figure 2. Most frameworks were published in the last two years. This is likely linked to the increasing use of IoMT in hospitals and the increasing number of cyber attacks. The work[27] published in 2021 is not listed in this section addressing RQ 1 because the operational risk management described here is also presented in newer work[15] published in 2022; see the justification in Study characteristics.

Frameworks Without Limitation to a Specific Threat

The study[15] discusses popular risk assessment methods and approaches (eg, OCTAVE, TARA, CVSS, Exostar, CMMI, ISO, NIST, FAIR) and their suitability for the IoMT. The authors conclude that their application fails in the case of the IoMT due to IoT specificities. The authors propose a new security risk management approach within e-health systems. It

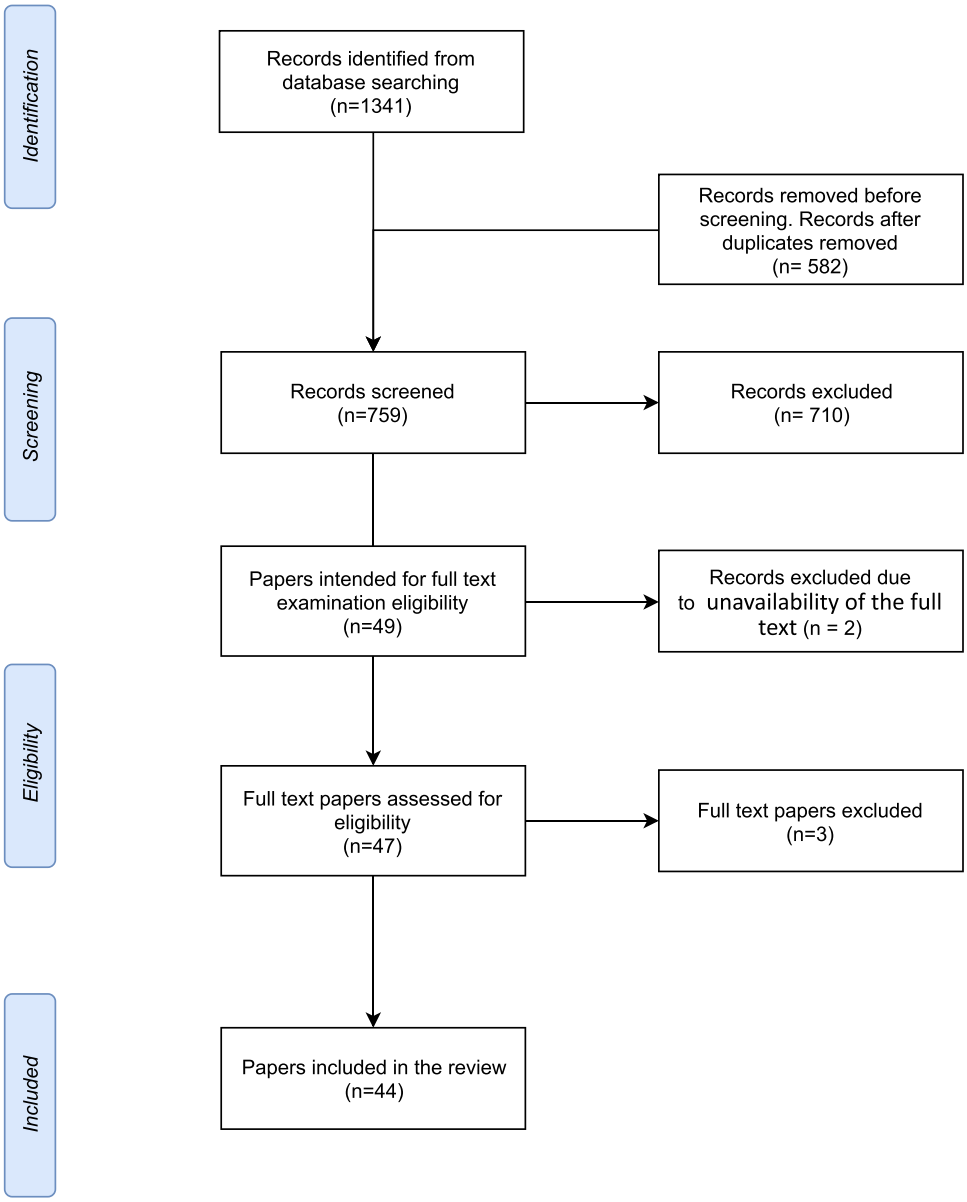

Figure 1 Flow diagram of selection of articles.

consists of three levels: data acquisition area, data gathering and transmission area and data processing and storage area. Their solution has a layered architecture containing a device risk manager, a network risk manager and a storage and processing risk manager, which are autonomous risk agents. Above these core modules is the core risk manager, which manages the risk database, addresses global risks and supports the individual modules. The risk management database contains information about users, devices, risk thresholds, etc. As possible sources of this information, the authors mention publications from organizations such as the FDA, NIST's NVD, and technical specifications from product suppliers. This information is used to identify abnormal behaviour.

Authors[28] describe a layered architecture using artificial intelligence and security methods (for example, cross-cutting services) for cyber-physical systems (CPS)-IoT enabled healthcare ecosystems. The work offers the conceptualization of the architecture and introduces components, which were implemented in different research projects. The work presents a proposal for simulation of the human cognitive behaviour to respond to new cybersecurity and privacy threats. The proposed architecture has four layers: collaborative, perception and knowledge, data collection and actuation, and

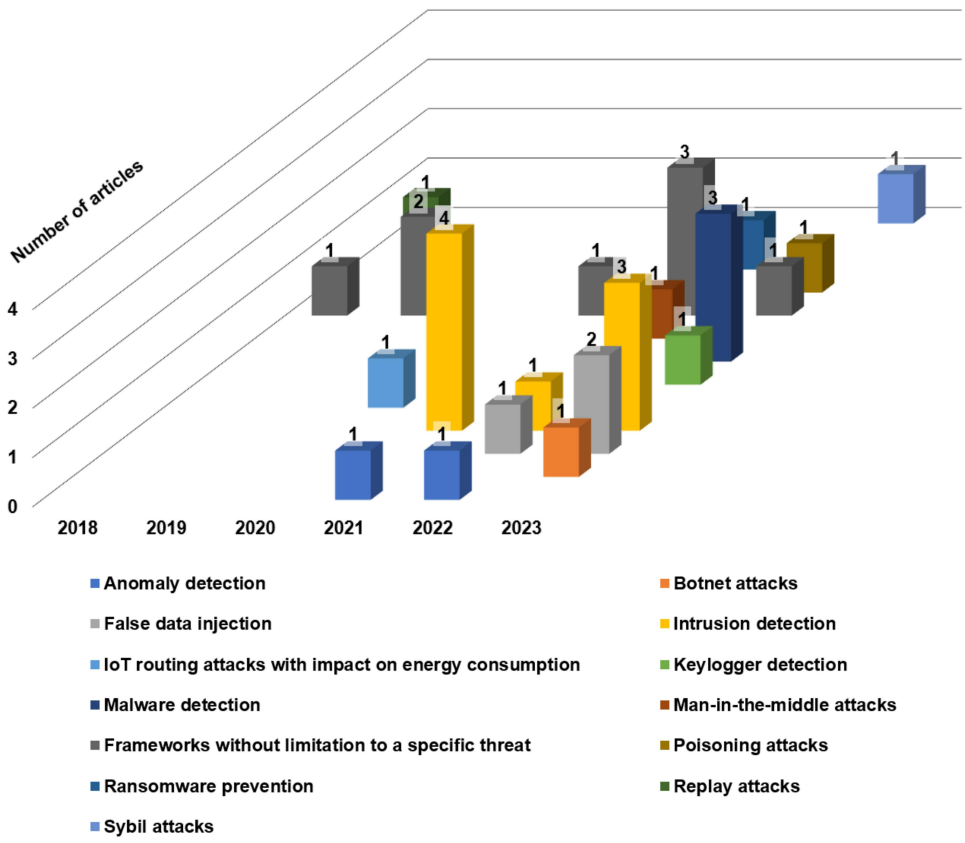

Figure 2 Publication year and focus of articles according to threat type (n = 32).

infrastructure. In the Perception and knowledge layer, a cognitive cycle security model is described with steps: Observe, Orient, Learn, Plan, Decide and Act. Models such as Bayesian networks or fuzzy logic are mentioned for the decision-making process.

The work[29] briefly describes a proposed framework of the layered-security model for IoMT. The model consists of perception, network, processing, analysis, and application layers. For each layer, the authors mention possible tools to secure the layer. Considered attack types are eavesdropping, node capture, fake node, denial of service, man in the middle, storage, malware, and malicious code. However, the paper does not provide a detailed description of the framework.

The paper[30] focuses on mitigating risks coming from unknown vulnerabilities of the IoT environment. The proposed method, Embedded policing and policy enforcement approach for future secure IoT technologies, is based on the principle of least privilege through the hardware security policy engine (SPE). SPE monitors the communication of applications. If suspicious access is detected, a predefined reaction is used to limit the attack. The system complements current authentication tools.

The framework[31] for reinforcing cybersecurity offers a solution for testing security threats and risks without the need to stop the system by using the Digital twins (DT) tool. DT allows the representation of the physical world, predicts risks, simulates cyber attacks, assesses the impact, and identifies threats and vulnerabilities in the IoT healthcare environment. The proposed framework can solve known vulnerabilities and threats. It consists of the physical world, DT world, and cybersecurity module. The cybersecurity module develops strategies using DT and updates the physical world module. The framework has automated processes: system modelling, testing/simulation and cyber threat prevention.

The aim of this work[32] is to integrate SecureIoT services in socially assisted robots usage scenarios for healthcare applications. It involves using two platforms: QTrobot for social interaction and teaching applications and CloudCare2U. SecureIoT platform offers open security services as Security as a service (SECaaS). It is a multi-layered security monitoring and enforcement system with the following layers: IoT systems, data collection and actuation, analytics, IoT security services, and use cases.

The authors[33] offer a novel IoMT framework for cyber-attack detection using the hybridization of Bayesian optimization and ELM to identify malicious access. It utilizes cloud architecture to mitigate cyber attacks in a real-time IoMT environment. The framework finds the optimal set of ELM hyperparameters and analyses the big data as a part of sensors and IoT devices.

Authors[34] propose an Improved wireless medical cyber-physical system (IWMCPS) framework, which consists of components and subsystems and can take into consideration all relevant security concerns. The system is based on ML techniques using a deep neural network for attack detection and classification. IWMCPS consists of the communication and monitoring core, computation and safety core, and real-time planning and administration of resources. The architecture of IWMCPS has four components: Data Acquisition Level, Data Aggregating Layer, Storing and Cloud Computing Level and Action Level.

Intrusion Detection

The work[35] describes a framework for intrusion detection in the IoMT environment regarding the privacy of patient data. Data from IoMT devices are stored in multiple cloud nodes with privacy protection. Sensitive data in nodes are identified, and an anonymization process is performed. Intelligent data fusion module adopts the contractive deep autoencoder with differential privacy. The module combines data from different sources and aggregates them. Quantum deep neural network is used to differentiate between normal and attack data.

The framework[36] proposes the IDS solution using deep learning and ML in fog-cloud architecture. A detection classifier is produced with a traffic processing engine and the ensemble learning combining a set of long short-term memory (LSTM) networks and a decision tree to identify normal and attack events. The authors presented a framework for implementing the proposed IDS in a fog-cloud architecture. The IDS is an Infrastructure as a Service (IaaS) in a cloud and Software as a Service (SaaS) in a fog.

The work[37] presents an Edge-IoT framework and prototype based on blockchain for smart healthcare applications. An optimized Crow search algorithm from the ML field is used for intrusion detection and tampering of data extraction. Secure application processing via blockchain is proposed. IoMT data are processed in the edge network, where a dataset is generated. The dataset is pre-processed, and the Principal component analysis feature selection algorithm reduces the dimension. A deep neural network is used for the processing of comparative analysis.

The proposed IDS framework[38] offers protection against malicious activities in IoT infrastructure. ML algorithms were used for intrusion detection: Logistic regression, Linear discriminant analysis, K-nearest neighbours, Gaussian naive Bayes, Classification and regression tree, Random forest, and AdaBoost. The main stages of the framework are: Data acquisition, Data handling and management, and IoT data classification for intrusion detection.

The proposed framework[39] uses blockchain technology to protect IoMT networks. IDS-chain contains distributed fog nodes to detect cyberattacks near the edge. There are three layers: IoMT device layer, IDS-based blockchain layer and cloud-based blockchain layer. The framework uses ML approaches to offer detection as a service (DaaS) in the fog layer and classification as a service (CaaS) in the cloud layer for attack classification and response management. Data exchange between IDS entities is secured by using blockchain.

Trustworthy intrusion detection model in e-healthcare systems[40] is a security tool for detecting malicious network traffic and helping to maintain patient health records safely. It uses an adaptive neuro-fuzzy inference system (ANFIS) to detect the unauthorized access of users. ANFIS-based data classification and if-then rule statements provide attack detection. Types of attacks are based on rule viewer, membership function and surface viewer. MATLAB framework is used for the practical implementation of the ANFIS model.

The Deep-learning model for detecting software defined healthcare IoT networks attacks (DeepDDoS)[41] focuses on the reflection type of DoS attacks. It is IDS, which uses historical data to train hybrid deep learning models. Vulnerable IoT devices are identified based on real-time generated traffic features. The model is loaded in a flask-script custom code at the gateway and performs prediction. Then, any suspicious traffic is forwarded through the control layer.

The solution presented in[42] uses an artificial neural network technique to predict suspicious devices. The mobility pattern is split into six parts and assigned to a specific slice. The solution uses a security module which monitors all clients connected to slices. MATLAB´s neural network was used to train data and detect and disable the problematic

device. The application can handle the four most applicable use cases: Life-critical services, Non-critical services, Suspicious devices, and Base station.

False Data Injection

The paper[43] states that conventional centralized threat detection systems (TDS) exhibit privacy issues because the central part of the TDS gains access to patients' physiological data. The online learning and attacking model using a recurrent deterministic policy gradient acquires patient data and generates FDI threat as an evaluation indicator to assess the system's vulnerability. The recommended method for deploying a decentralized threat detector to deter an attack is deep optimized attentive federated aggregation (DpOptFedAA), where the TDS is trained on patient controller modules. The controllers do not share the physiological data, and the hospital server cannot access them. It performs the aggregation and returns the updated parameters. A gated recurrent unit model is used for threat detection.

The introduction to the article[44] discusses related works focusing on measurement manipulation attacks, excluding machine learning-based models. However, none of the reported works can identify real-time vulnerable measurements. Based on this finding, the authors propose a personalized health analyser for security enhancement (PHASE), which can perform real-time security analysis of a personalized smart healthcare system (SHS). It consists of three components. The essential part is a knowledge base with patient status inference rules and time-series verification rules. The optimizer component (based on the satisfiability modulo theorem) generates optimal attack vectors. These are passed to the checker component to assess the vulnerability of the measurements. A PHASE-generated vulnerability report output reports the results to the healthcare provider and data analysts.

The authors[45] present a new resilient security framework based on the ML approach combined with blockchain technology. A tri-layered neural network (TNN) is used to detect malicious data from medical sensors. In case of detection of cyberattacks, such data are not processed at the fog layer. Data after confirmation are transmitted into the fog layer with blockchain technology to ensure data integrity.

Malware Detection

The proposed TSDroid framework[46] is focused on Android malware detection. The majority of healthcare devices use the Android operating system. A novel Android malware detection framework is presented in the article. The method proposes clustering based on temporal and spatial metrics. The life cycle of API is used as a temporal metric, and the size of API is used as the spatial metric. Four algorithms are used to determine the optimal algorithm and optimal cluster number. A time series-based clustering algorithm is used to create subsets and improve detection capability.

The aim of the work[47] is to propose a method for identifying files containing malware and pirated software using integrated deep logic. A hybrid dual-channel convolution neural network with spider monkey optimization is a combination of optimization-based deep learning techniques for detecting software piracy. It uses software plagiarism to detect the features of original software. The raw data files are first pre-processed. Frequency and inverse document frequency and logarithm-term frequency are weighting algorithms used to find similarities in source codes. Then, the detecting module checks the pre-processing data. The method can identify ransomware and counterfeit threats by studying the signatures in datasets. The system administrator receives a notification. Malicious file formats are highlighted in a colour to demonstrate the malware's characteristics.

The paper[48] proposes a Many-objective optimization-driven data balancing strategy for cross-architectural malware classification (MODSC). MODSC offers the optimization problem model for data balancing strategy search based on dataset information. The model rebalances the data space in different dimensions to solve multidimensional data imbalance with category and architectural distribution. The model is solved by a many-objective evolutionary algorithm.

Anomaly Detection

The work[49] proposes a smart digital healthcare system using supervised ML models called Bio-inspired optimization for classification and anomaly detection (BIOCAD). Supervised ML models are used for disease classification, and unsupervised ML is used for anomaly detection to prevent manipulation with sensor measurements. BIOCAD

optimization framework is proposed for data classification and anomaly detection. Historical patient vital signs data are used to train learning models. It consists of two parts: classifier and anomaly detector, and bio-inspired optimization module.

Deep neural network-based classification and anomaly detection (DeepCAD) is a framework[50] that uses a deep neural network (DNN) model integrated with anomaly detection in SHS. The model performs two feature classification and anomaly detection. Into the DNN model are added anomaly detection rules. The framework consists of two steps: data processing and model training.

Botnet Attacks

The authors[51] offer a methodology that helps secure IoT devices thanks to the early detection of IoT Botnet attacks. ML models are used for detecting botnet attacks. Small chips are integrated into IoT devices to secure the healthcare processes. The chips contain a training model and receive data packets, and if a malicious packet is detected, the originator is blocked from the healthcare system and alerts are sent to a security administrator. As part of the solution, a random forest classifier is proposed.

Keylogger Detection

The methodology[52] presented in the paper focuses on keylogger attacks that can compromise private information and cause operational problems in the IoT environment. A nano-integrated circuit (NIC) is used for IoT devices. It recognises malicious packets with keylogger attack detection trained ML models. NIC acts as the data packet receiver with the identical hardware configuration of an actual IoT device. Then, it decides if a packet can be allowed for communication.

Man-In-The-Middle Attacks

The paper[53] proposes a framework for detecting and mitigating Man-in-the-middle attacks. The system detects data modification which is caused by this type of attack. It consists of entities: client, server and intermediate servers. The attack modifies the data from the client. Detection is based on checksum. Each record is connected to a unique checksum calculated using the SHA256 function. The correctness of the data is validated using checksum. For mitigation, alternate routing is used. Only correct data is accepted at the server end.

Poisoning Attacks

The proposed framework[54] is based on blockchain-based federated learning and secure multi-party computation model verification against poisoning attacks. System architecture contains hospitals, cloud, and private blockchain network. ML local models of hospitals are checked and verified. Then, models are aggregated to the blockchain node. The global model is distributed to hospitals that are joined in federated learning.

Ransomware Prevention

The proposed framework architecture[55] allows ransomware analysis with detection and validation. It uses capabilities such as identification, monitoring and alerting of abnormal sourcing patterns for incident response. A detection filter can recognize ransomware attacks (static and dynamic) and measure damage to IoMT devices. The validity and accuracy of attacks are performed by a comprehensive verification process. This defence solution was developed to block attacks and notify the base station.

Replay Attacks

The authors[56] suggest a framework for detecting replay attacks on battery depended IoT devices. The framework combines a universally unique identifier, timestamp and a self-learning battery depletion monitor. Data collected from IoT devices are sent from the microcontroller to the IoT cloud platform as well as the battery level. A replay attack detection framework provides decisions about unusual behaviour. In case of an attack detection, the system based on the framework sends a warning message to the healthcare staff.

Sybil Attacks

Blockchain-based fuzzy trust (BFT-IoMT) management framework[57] is proposed for the detection of Sybil nodes in the IoMT environment. The architecture consists of an IoMT/infrastructure layer and a fog layer. The fog layer works with details from the IoMT layer and uses modules to detect nodes, cluster, and calculate trust. For trust assessment of nodes, fuzzy logic is used. Node services are stopped if the trust value is below the threshold and a node asks for communication. Malicious nodes are isolated.

IoT Routing Attacks with Impact on Energy Consumption

To prevent destroying the entire network, this framework[58] helps detect, predict and mitigate the impact of IoT routing attacks on power consumption in real-time. The model architecture is proposed for healthcare for the elderly at home. Three phases are provided: medical data collection, routing, network, and medical application layers. The model uses deep learning to create a robust model and high-performance metrics. The used deep learning tool is a convolution neural network to predict and detect IoT routing attacks that impact energy consumption and can destroy the network.

Advances in the design of security frameworks for evaluating the security level of information systems using IoMT in healthcare

To answer RQ 2, the review included twelve papers describing frameworks for risk assessment in the context of IoMT use. Ten frameworks offer an assessment of the current IoMT environment, and two of the ten also allow a comparison of possible IoMT acquisition alternatives. One paper focuses on the evaluation of possible IoMT acquisition alternatives only,[59] and one framework proposes testing of security IoMT devices that can be used by manufacturers.[60] Eight of the twelve papers explicitly mention that their solutions address privacy concerns. None of the frameworks offer an assessment of organisational measures.

The paper[27] proposes dynamic agent-based risk management. This context-aware agent-based risk management model for IoMT environments relies on a hybrid (qualified and quantified) risk assessment. The model is applicable to operational risk management or analytical risk management. The framework divides the system into zones of common risk factors. Cyber risk management consists of a device risk management agent, a network risk management agent, and a storage and processing risk management agent. Each agent estimates and shares the risk rating with the central part of the cyber risk management. The system administrator defines the initial risk threshold for anomalies and suspicious scenarios. The user, architect or administrator defines threat impacts. The likelihood of anomalies is evaluated at each level separately using parameters such as the readiness of the medical device to detect and respond to an attack, lack of security awareness in the user, device criticality, openness to the internet, protocols security and others. The authors state that this method can be used to evaluate both attacks on one and many devices. Thus, it is possible to compare medical devices from different manufacturers using this method.

The authors of[59] present a multicriteria decision-making method for IoMT device assessment and selection, which is a framework of identified security attributes. Related works mainly working with analytical hierarchical processes and techniques for order preference by similarity to ideal solution (TOPSIS) methods are mentioned. For each, a list of security requirements – attributes used are collected. Based on ISO standards, 13 criteria (attributes) are defined. The framework assesses each alternative in terms of the security attributes. The process continues with the TOPSIS method, which determines the ranking of the alternatives according to their suitability.

In the paper,[61] the authors conclude from a study of related works that no tool is available that covers all IoMT-related security scenarios and does not require technical expertise on the user's part. Such a tool would allow stakeholders to identify potential security issues and recommend countermeasures, assess the suitability of different IoMT solutions and select the most suitable one from a security perspective. The authors propose a Python web application consisting of recommendation and evaluation modules. The recommendation module works based on inputs that include information about the stakeholder type, IoMT solution, device type and architecture. It then runs a process identifying security issues and recommending actions for each component related to the embedded IoMT solution. Then, the output step categorizes the potential problems and recommends a set of attributes (in the form of yes/no questions) for their countermeasures.

The evaluation module assesses the security level of different solutions and compares them. A quantitative assessment method based on the analytic hierarchy process is used to assess the security level of each solution.

The paper[16] first critically analyses existing popular cybersecurity frameworks (OCTAVE, TARA, NIST, ISO). According to the authors, their extension to IoT environments cannot cover new security risks related to IoT specifics. A new method for risk score computing for the IoT is presented to enable the classification and quantification of IoT risks. The aim is to enable the determination of the risk level of individual IoMT devices. The risk is calculated for each device as the product of the risk impact and the likelihood of the risk. The following parameters are considered to calculate the risk impact: network type, protocol type, number of heterogeneous systems involved, device security, confidentiality, integrity and availability type. The weights for each parameter and the impact calculation are presented. The following parameters are considered to calculate the probability of risk: the number of past attacks for the device, the IoT layer that undergoes lots of attacks, the type of sector using the IoT, and the device risk factor (for the IoMT only). The calculation for the probability is also presented, and the weights for each parameter are introduced. Based on the risk rank range, the resulting value shows whether the risk is very low, low, medium, high or very high.

The paper[62] presents iCerberus, the framework for representing IoT security and privacy policies and detecting policy issues. It consists of an ontology for modelling IoT security and privacy policies iCerberus, policy editor iCerberux, policy notation iCerbac, guidelines and rules for detecting IoT policy errors. It is a web-based administration tool to specify, analyze, modify and test policies to detect errors. Reviewing and validation are performed against pre-defined policies.

The author[63] presents the Refinement Risk Loop method, which combines secure system design with risk assessment. It uses the Isabelle infrastructure framework with attack trees to improve the system's security. Isabelle infrastructure framework, a generic higher-order logic proof assistant, allows modelling of physical and logical elements and provides attack trees. The process is iterative and refines a system specification. Existing risk assessment loops use generating attacks to plan incident responses. The proposed method uses risk assessment to refine the design of a secure system.

The proposed model[64] used the Control objectives for information and related technology (COBIT 5). It consists of three parts: Healthcare IoT risk management, Hospital performance indicator for accountability (HPIA) alignment and COBIT 5 implementation phases. Hospital Kuala Lumpur was chosen as a case study. The first part of the model is COBIT IoT risk management, which incorporates HPIA categories (for example, customer focus, employee satisfaction, financial and office management). Finally, seven phases of implementation from COBIT 5 are used.

The proposed[65] model is based on The Decision-making trial and evaluation laboratory (DEMATEL) procedure of IoT risk assessment. As a case study, the RC Hospital in Sudan was chosen. The aim is to help IT security improve IoT architecture and mitigate technology risks to ensure patient safety considering risk categories: secured technology, human privacy and trustable processes and data. There are five steps: setting goals, technology risk evaluation, reassure improvement and innovation, facilitating transformation, and common process. The authors mention the importance of continuous improvement and updating IoT infrastructures. The transformation step also mentions the importance of hospital staff training in ICT technology.

The authors[66] propose a novel multi-security and privacy benchmarking framework for blockchain-based IoT healthcare industry 4.0 Systems. The proposed multi-criteria decision-making benchmarking framework introduces the combination of the GRA-TOPSIS and the BEZ optimization method for benchmarking of systems and a new extended fuzzy weighted with zero inconsistency (FWZIC) method, which is spherical FWZIC (S-FWZIC) for weighting the involved criteria. The first phase formulates a decision matrix (ie access control, integrity availability). In the second phase, S-FWZIC method calculates the weights of each from security and privacy properties and the system solutions are ordered by similarity to the ideal solution.

The paper[24] introduced the IoT Security Risk Model for Healthcare based on the ISO/IEC 27005:2018 standard establishing the context of IoT risk in healthcare. The model is used for an iterative IoT risk management process, and at each iteration, it increases the depth and detail of the assessment until it reaches the acceptance level. IoT is described in five layers with technology assessment: authentication, encryption, secured boot, intrusion prevention system and firewall, education and policies. The authors mention all IoT users (also patients) in the education layer. As a case study, Hospital Kuala Lumpur was used.

Threat and risk management (TMR) framework for eHealth IoT systems[67] is based on STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) and LINDDUN methodologies. These are used for the assessment of a single configuration of an architecture. The TMR will help manage the security and privacy of systems with many feature combinations in the IoT healthcare environment. Compared to the two mentioned methodologies, TMR includes components on feature space modelling, threat assessment of consequent risks, risk-driven scoring, support of configuration decision and regulatory compliance. The article describes the current status of proposed framework development. The author expects to present further progress in future publications.

The authors[60] offer a new framework for testing the security of IoT devices. The framework is based on the Open web application security project (OWASP) IoT framework, which is extended with three additional parts: IoT security considerations, which include mapping of vulnerabilities to a set of security tests (selection of tests), Methodologies and tools with mapping of tests to useful tools to perform tests, and Threat models describes detailed threat modelling. It is mentioned that security frameworks for IoT should be continuously updated; nevertheless, the OWASP attack surface mapping has not been updated since 2015. IoT producers should test their products to decrease security vulnerabilities.

Discussion

Principal Findings

This scoping review aimed to present what progress has been made in recent years in the area of risk management research and security assessment for information systems incorporating IoMT devices. Based on the identified studies, it can be concluded that there are only a limited number of proposed solutions for evaluation of possible IoMT acquisition alternatives and none of the studies found looked at the assessment of organisational measures. Since it concerns the use of information technology in healthcare, which is one of the key sectors, further research is needed to cover this area. Most of the studies mentioned above point out the specificities of the IoMT, such as the heterogeneity of devices,[16,28,35,37,57] the rapid development and proliferation of new devices,[28,35,36,45,56] the large amount of sensitive data exchanged wirelessly,[34–36,56] the layered architecture[15,28,29,31,32,45,56,57] and the multitude of users who often lack security awareness.[23,24,27]

It is important to note that this review focused only on finding and describing thematically relevant work and then answering the research questions. It did not engage in a formal evaluation of the research methods used, nor did it focus on the deeper comparison of the solutions presented by the authors.

RQ 1 aimed to identify progress in designing security frameworks for IoMT risk assessment and management and their proposed technology solutions. Limitation to a specific threat is not mentioned in the eight works. Eight frameworks are focused on intrusion detection. Three papers are related to false data injection, three to malware detection and the rest are individual focuses. Several solutions addressed a specific type of attack: manipulating sensor measurements (eg, blood pressure or glucose).

The critical issue is the high risk of potential threat to patient health and life with subsequent medication based on incorrect measurement values. Therefore, designed frameworks are dedicated to detecting the attack and providing a risk response to mitigate the impact. In this regard, let us mention three solutions. The paper[43] proposes to account for the privacy problem in its solution and does not allow the sharing of patient physiological data from sensors with the central part of the TDS. On the other hand, the paper[44] emphasizes real-time control of sensor measurements. Moreover, it provides guidance on the selection of the most important measurements that should be protected. The framework[45] suggests a combination of detection of malicious data from medical sensors using TNN and blockchain technology for secured data transmission.

From the point of view of used methods and technologies, ML methods seem to be a game changer in detecting malicious intrusion. From thirty-two identified frameworks in subsection Advances in security frameworks for risk assessment and management for IoMT, twenty-two works use ML techniques in different variations. Five works suggest using blockchain technology, four of which combine blockchain technology with ML techniques.

As a result of the search of studies, only one work[15] was identified that focuses on the comprehensive assessment and management of different risks in IoMT operations. The framework works at the level of the different layers of the IoMT environment (device, network, storage), which are managed by the modules responsible for their control. Then, the risk

assessment also occurs at the global level. The study builds on the finding that established standard general frameworks cannot be successfully applied due to the specificities of the IoMT environment. One of the key parts of the proposed framework is the risk management database. The authors generally mention the content and state that the database should contain all available information related to the IoMT. The database contains, among other things, initial thresholds for each abnormality. According to the authors, these should be entered by a security architect. As in the case of the framework,[61] including security-specific information from IoMT device manufacturers is expected to be time-consuming to obtain and insert. There is also the issue of continuously developing new threats and incorporating them into risk management on time. Thus, building a regularly updated general risk management database for the IoMT could be the next direction for researchers.

RQ 2 aimed to determine the state of research in developing security frameworks for assessing the level of information system security in healthcare facilities (hospitals) in conjunction with the use of the IoMT. Such frameworks may include an assessment of organisational security measures. Studies identified during the selection process focused on helping users with decision-making when choosing between IoMT device alternatives. The assessment of alternatives occurs through defined attributes. In the case of the works[61] and,[59] the user is required to fill in answers to questions related to the attributes (eg, authorization, secure key management). The output of the assessment process is a ranking of the suitability of the alternatives. Given the need to obtain data from manufacturers, the authors of[61] plan to involve device manufacturers in defining the security of their solutions and sharing more technical details. The framework's authors[60] mention manufacturers' lack of testing of IoMT devices and offer a test guide to assess the level of security.

Two frameworks[16,27] assess the level of risk as a combination of the impact of the threat and the probability of the threat occurring. However, Ksibi et al[27] do not offer guidance for determining the threat impact value. The authors state that the user, architect or administrator defines threat impact. They then offer several examples of calculating the probability for each layer of the IoMT environment. In addition, the framework[16] defines parameters for determining the impact value and the threat probability, as well as the weights for each of their levels. In this case, the PIER model proposed for connected and autonomous vehicles[68] could be an inspiration for risk-level assessment. The model works with a combination of probability (P) and impact (I) but complements the assessment with the categories exposure (E) and recovery (R).

Some authors updated or extended existing standards or frameworks for use in IoMT environments; these are COBIT 5,[64] ISO/IEC 27005:2018,[24] DEMATEL,[65] STRIDE and LINDDUN.[67] Although blockchain technology is significantly expanding in health information systems, only one framework[66] has been published to assess the security and privacy focuses on information systems using blockchain technology. The Refinement-Risk-Loop method,[63] focusing on insider threats, which uses logical models to plan the security structure in individual iterations, allows the infrastructure to be assessed and the target security level to be planned. The authors mentioned that formal blockchain models are unavailable in used infrastructure tools.[63]

No framework was found within the included frameworks that evaluate an information system's overall security level containing many different IoMT devices, focusing on IoMT-specific threats. Furthermore, although several papers mention the issue of the number of IoMT users with low awareness of information system security, no framework was found that focused on addressing this issue. None of the frameworks offers an assessment of organisational measures despite the fact that the importance of the organization measures was already highlighted. For example, the paper[22] describes the impact of the organizational structure of hospitals on departments of medical technology (MT) and information technology (IT). MT department, responsible for medical devices, should be strongly connected to the IT department or merged. Only in this case can they cover the requirements of operating IoMT devices and security concerns. The authors mentioned that cyber attacks were successful only in hospitals with separated departments.

Fifteen papers explicitly mention that their solutions also address privacy concerns; seven are included in RQ 1 and eight in RQ 2. The use of blockchain (e.g.[45]) has been cited as a solution to the problem of maintaining data privacy. In the case of sensor data, privacy protection is used by the anonymization process for sensitive data from cloud nodes.[35]

New or upcoming regulations and standards may have an impact on IoMT security or may be used within IoMT security frameworks. In terms of security implications, there are new challenges within the European Union arising from the Proposal for a regulation – The European Health Data Space (EHDS),[69] and the Data Act.[70] The EHDS seeks, among other things, to ensure data sharing "a consistent, trustworthy and efficient set-up for the use of health data for research, innovation, policy-making and regulatory activities".[69] The authors of an article[71] examining the impact of new and

forthcoming European Union legislation state that health data sharing, despite anonymisation, poses a risk of patient re-identification. This is a lack of risk assessment on the part of data access bodies. The related Data Act[70] sets out the obligations and rights for sharing data generated by an IoT medical device between data holders, users, third parties and governments. Data holders can be device manufacturers or healthcare providers. For IoT devices, there is an obligation to design them so that the data generated by the device are directly accessible to the user, if technically feasible. This obligation will come into force on 12 September 2026.[70] Possible impacts of this requirement include cybersecurity, increased computing power of the device and shorter battery life. Data sharing presents new obligations and challenges for data holders.[72] This area should be explored for possible inclusion in IoMT security frameworks.

Two FDA initiatives are of interest from the perspective of use within IoMT frameworks. Draft guidance Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the FD&C Act,[73] which lists forthcoming updated recommendations for cyber devices. It contains recommendations for manufacturers that include updating plans and procedures for identifying, monitoring, and addressing cyber threats when a new threat, risk, is identified throughout the lifecycle. Updating from the perspective of new threats would allow for increased security of devices, but it is necessary to ensure that the database of each framework[15,61] is updated. Another initiative is a review of approaches and recommendations for future cybersecurity risk management of legacy medical device prepared by The MITRE Corporation for the FDA.[74] These are resources that are still fit for purpose, but their security may no longer meet current requirements. Planned research includes exploring the perspectives of both manufacturers and medical devices, sharing technical information, and developing new policies to address the cybersecurity of legacy devices.[74] This initiative could provide support for improving security assessment of IoMT environments containing legacy medical devices.

The IEEE organization states that the IEEE2621 Standards for Wireless Diabetes Device Security Assurance are applicable to all medical devices. These standards provide support to manufacturers for identifying threats, defining security requirements, ensuring the security of connected devices, and interfacing with users' mobile devices.[75] To assess compliance with these standards, IEEE offers the Medical Device Cybersecurity Certification Program,[76] prepared to help manufacturers test their devices from a cybersecurity perspective. Although these standards are focused on diabetes devices, as stated by the IEEE, the standards can be extended to other medical devices. Thus, certification could be included as part of frameworks for assessing the suitability of alternative devices. The forthcoming new standard IEEE P2933 – Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS – Trust, Identity, Privacy, Protection, Safety, and Security[77] addresses ensuring the ethical use of technology in healthcare settings. The standard will cover not only the development and production of medical devices, but also, for example, the area of user interaction.[77] It could therefore be a valuable resource for IoMT security frameworks.

The design of a generic risk management database to be used by IoMT security frameworks could draw on information sources gathered by organizations and initiatives such as NIST, FDA, H-ISAC, IEEE and others. It can be anticipated that these sources will ensure the inclusion of the latest threats and vulnerabilities in regular updates. Thus, these sources could be used to create an overview of the cyber risks associated with the use of IoMT. Another part of the database should be an overview of individual IoMT devices and technical specifications related to cyber security and assurance. The source could be the data provided by the manufacturer during product registration, eg the EUDAMED database. Unfortunately, its full launch is estimated for 2027.[78] The database will not include older devices, and registration will only be mandatory in the event of a serious adverse event.[79] The completeness of the database appears to be problematic due to the lack of documentation for older devices and also in terms of possible new threats and vulnerabilities that were not known at the time of registration. FDA initiatives are attempting to address these points.[74,75] The provision of cyber threat protection by IoMT manufacturers cannot cover some threats and vulnerabilities that result from incorporation into the healthcare device environment, such as device hijacking, phishing, or DoS. If the database is to be used by healthcare facilities to provide an assessment of all security-related aspects of the IoMT environment, it should also include a set of legislative requirements imposed on healthcare providers, such as initiatives within the EU,[69,70] for which adequate security must be ensured. For all parts of the database, the question remains how to ensure regular updates and their frequency.

Limitations

There are several limitations to this review. One is the limited number of databases searched, and grey literature was not examined. Regarding search terms, it is possible that other alternative names for IoMT or IoT for healthcare resources were not covered. At the same time, only papers published in English were included. All these facts could have led to a distorted result of the answers to the RQs. Besides, the review protocol was not registered.

It is also important to mention that a scoping review, as a specific type of overview, does not, by its very nature, provide a deep insight into the investigated area like a systematic literature review, as it has a different goal and purpose. A scoping review primarily provides a basic overview of the thematic coverage of the investigated area and identifies research gaps.[7] Therefore, the authors focused primarily on the solution description, evaluation, limitations, and future work for the individual articles included in the scoping review. The above can be considered a limitation of the article.

Conclusions

As described in the introductory section, many papers focus on identifying and describing security and privacy threats specific to the IoMT domain. Also, several papers are dedicated to finding solutions to mitigate the impact of each threat and defend against threats. There are also works that address a specific security threat. On the other hand, significantly fewer studies address security frameworks for overall risk assessment and management for the IoMT and related issues. Therefore, it can be argued that there is a research gap for future research in the area of risk management and security assessment for information systems in environments involving IoMT devices.

The contribution of this scoping review is the description of the current state of research and the identification of the understudied area of risk assessment and management for the IoMT. Research should focus on developing frameworks for operational security risk management at all levels of the IoMT environment, not only in general terms but also in designing specific technology solutions. The review also presented current options for assessing IoMT alternatives from a security perspective to stakeholders involved in the selection of IoMT solutions. At the same time, it pointed to the scope for further research focus, namely frameworks for assessing an information environment's overall security and privacy level with many IoMT devices, including its architecture layers (perception, network, and application layer). The research should include assessment not only from a technological perspective but also from a sociotechnical perspective. Moreover, a possible area of further interest for researchers could be the design of a regularly updated general risk management database for the IoMT, which could be further used in designing risk management frameworks for IoMT environments.

Only fifteen works have also addressed privacy concerns, usually in conjunction with the use of blockchain technology. From a privacy perspective, addressing privacy concerns must be an integral part of the proposed security frameworks in healthcare. As the Introduction section mentions, security and privacy concerns are intertwined, and cyber attacks can target privacy breaches. In this regard, blockchain technologies are very promising. An example can be the blockchain hyperledger fabric-enabled IoMT distributed architecture using NuCypher Re-Encryption mechanism to ensure higher security, the secrecy of records, and medical ledger integrity and transparency.[80] However, even such solutions must always be supported by organizational security measures.

Funding

The work was supported by an internal funding mechanism provided by the Prague University of Economics and Business (F4/1/2023; IP400040).

Disclosure

The authors report no conflicts of interest in this work.

References

1. Premalatha V, Sreedevi EP, Sivakumar SS. Contemplate on internet of things transforming as medical devices - the internet of medical things (IOMT). In: Proceedings of the 2019 International Conference on Intelligent Sustainable Systems. New York: IEEE; 2019:276–281. doi:10.1109/iss1.2019.8908090.
2. Dimitrov D. Medical internet of things and big data in healthcare. *Healthcare Infor Res*. 2016;22(3):156. doi:10.4258/hir.2016.22.3.156

3. Dwivedi R, Mehrotra D, Chandra S. Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: a systematic review. *J Oral Bio Craniofacial Res*. 2022;12(2):302–318. doi:10.1016/j.jobcr.2021.11.010
4. Prasad VK, Solanki J, Bhattacharya P, Verma A, Bhavsar M. Artificial intelligence applications for IoMT. In: *Federated Learning for Internet of Medical Things*. CRC Press; 2023.
5. Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener Comp Syst*. 2018;82:395–411. doi:10.1016/j.future.2017.11.022
6. Karie NM, Sahri NM, Yang W, Valli C, Kebande VR. A review of security standards and frameworks for IoT-based smart environments. *IEEE Access*. 2021;9:121975–121995. doi:10.1109/access.2021.3109886
7. Munn Z, Peters MDJ, Stern C, Tufānaru C, McArthur A, Aromataris E. Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. *BMC Med Res Meth* 2018;18(1). doi:10.1186/s12874-018-0611-x
8. Vaiyapuri T, Binbusayyis A, Security VV. Privacy and trust in IOMT enabled smart healthcare system: A systematic Review of current and future trends. *Int J Adv Comp Sci Appl*. 2021;12(2):731–737. doi:10.14569/ijacsa.2021.0120291
9. Hatzivasilis G, Soultatos O, Ioannidis S, Verikoukis C, Demetriou G, Tsatsoulis C Review of security and privacy for the internet of medical things (IoMT) resolving the protection concerns for the novel circular economy bioinformatics. In: 2019 15th International Conference on Distributed Computing in Sensor Systems. New York: IEEE, 2019:457–464. doi:10.1109/DCOSS.2019.00091.
10. Garg N, Wazid M, Singh J, Singh DP, Das AK. Security in IoMT-driven smart healthcare: a comprehensive review and open challenges. *Security and Privacy*. 2022;5(5):e235. doi:10.1002/spy2.235
11. Yaqoob T, Abbas H, Atiquzzaman M. Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review. *IEEE Communic Surveys Tutorials/IEEE Communi Surveys Tutorials*. 2019;21(4):3723–3768. doi:10.1109/comst.2019.2914094
12. Majdoubi DE, Bakkali HE, Sadki S, Maqour Z, Leghmid A, G TR. The systematic literature review of privacy-preserving solutions in smart healthcare environment. *Secur Commun Networks*. 2022;2022:1–26. doi:10.1155/2022/5642026
13. Bhuiyan MN, MdS R, Billah M, Saha D. Internet of things (IoT): a review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. *IEEE Internet Things J*. 2021;8(13):10474–10498. doi:10.1109/jiot.2021.3062630
14. Almolhis N, Alashjaee AM, Duraibi S, Alqahtani F, Moussa AN The security issues in IoT - cloud: A review. In: 2020 16th Ieee International Colloquium on Signal Processing & Its Applications. New York: IEEE; 2020:191–196. doi:10.1109/CSPA48992.2020.9068693.
15. Ksibi S, Jaïdi F, Bouhoula A. A comprehensive study of security and cyber-security risk management within e-health systems: Synthesis, analysis and a novel quantified approach. *J Spec Topics Mobile Net App*. 2022;28(1):107–127. doi:10.1002/spy2.235
16. Kandasamy K, Srinivas S, Achuthan K, Rangan V. IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP J Inform Secur*. 2020;2020(1). doi:10.1186/s13635-020-00111-0
17. Rana K, Singh AV, Vijaya PA A systematic review on different security framework for IoT. In: 2018 Fifth International Symposium on Innovation in Information and Communication Technology. New York: IEEE; 2018:39–44. doi:10.1109/ISIICT.2018.8613296.
18. Sultan A, Mushtaq MA, Abubakar M IOT security issues via blockchain: A review paper. In: 2019 International Conference on Blockchain Technology. New York: ACM; 2019:60–65. doi: 10.1145/3320154.3320163.
19. Wei Z, Cao C, Huo D, et al. Reviewing IoT security via logic bugs in IoT platforms and systems. *IEEE Int Things J*. 2021;8(14):11621–11639. doi:10.1109/jiot.2021.3059457
20. Alshohoumi F, Sarrab M, AlHamadani A, Al-Abri D. Systematic review of existing IoT architectures security and privacy issues and concerns. *Int J Adv Comput Sci Appl*. 2019;10(7):232–251. doi:10.14569/ijacsa.2019.0100733
21. Ghafur S, Kristensen SR, Honeyford K, Martin G, Darzi A, Aylin P. A retrospective impact analysis of the wannacry cyberattack on the NHS. *Npj Digital Med*. 2019;2(1). doi:10.1038/s41746-019-0161-6
22. Willing M, Dresen C, Haverkamp U, Schinzel S. Analyzing medical device connectivity and its effect on cyber security in German hospitals. *BMC Med Inf Decis Making*. 2020;20(1). doi:10.1186/s12911-020-01259-y
23. Branch LE, Eller WS, Bias T, et al. Trends in Malware attacks against United States healthcare organizations, 2016-2017. *Global Biosecur*. 2019;1(1):15. doi:10.31646/gbio.7
24. Bakar NAA, Ramli WMW, Hassan NH. The internet of things in healthcare: an overview, challenges and model plan for security risks management process. *Indo J Electr Eng Comp Sci*. 2019;15(1):414. doi:10.11591/ijeecs.v15.i1.pp414-420
25. Tricco AC, Lillie E, Zarin W, et al. PRISMA extension for scoping reviews (PRISMA-SCR): Checklist and explanation. *Ann Internal Med*. 2018;169(7):467–473. doi:10.7326/m18-0850
26. Rayyan - AI powered tool for systematic literature reviews [homepage on the internet], 2023. Available from: https://www.rayyan.ai/. Accessed April 07, 2024.
27. Ksibi S, Jaidi F, Bouhoula A Cyber-risk management within IOMT: A context-aware agent-based framework for a reliable e-health system. In: The 23rd International Conference on Information Integration and Web Intelligence. New York: ACM; 2021:547–552. doi:10.1145/3487664.3487805.
28. Abie H Cognitive cybersecurity for CPS-IoT enabled healthcare ecosystems. In: International Symposium on Medical Information and Communication Technology. New York: IEEE; 2019:216–221. doi:10.1109/ismict.2019.8743670.
29. Rizk D, Rizk R, Hsu S Applied layered-security model to IoMT. In: 2019 IEEE International Conference on Intelligence and Security Informatics. New York: IEEE; 2019:227. doi:10.1109/ISI.2019.8823430.
30. Siddiqui F, Hagan M, Sezer S Embedded policing and policy enforcement approach for future secure IoT technologies. In: Living in the Internet of Things: Cybersecurity of the IoT. IET Conference Publications; 2018. doi:10.1049/cp.2018.0010.
31. Pirbhulal S, Abie H, Shukla A H. Towards a novel framework for reinforcing cybersecurity using digital twins in iot-based healthcare applications. In: IEEE Vehicular Technology Conference VTC. New York: IEEE; 2022. doi:10.1109/VTC2022-Spring54318.2022.9860581.
32. Vulpe A, Crăciunescu R, Drăgulinescu A, Kyriazakos S, Paikan A, Ziafati P. Enabling security services in socially assistive robot scenarios for healthcare applications. *Sensors*. 2021;21(20):6912. doi:10.3390/s21206912
33. Nayak J, Meher SK, Souri A, Naik B, Vimal S. Extreme learning machine and Bayesian optimization-driven intelligent framework for IoMT cyber-attack detection. *J Supercomp*. 2022;78(13):14866–14891. doi:10.1007/s11227-022-04453-z
34. Alzahrani AA, Alshehri M, AlGhamdi R, Sharma SK. Improved wireless medical cyber-physical system (IWMCPS) based on machine learning. *Healthcare*. 2023;11(3):384. doi:10.3390/healthcare11030384

35. Al-Hawawreh M, Hossain MS. A privacy-aware framework for detecting cyber attacks on internet of medical things systems using data fusion and quantum deep learning. *Info Fusion*. 2023;99:101889. doi:10.1016/j.inffus.2023.101889
36. Khan F, Jan MA, Alturki R, Alshehri MD, Shah ST, Rehman AU. A secure ensemble learning-based fog-cloud approach for cyberattack detection in IOMT. *IEEE Trans Ind Inform*. 2023;19(10):10125–10132. doi:10.1109/tii.2022.3231424
37. Alshammari N, Syed T, Syed MB. An edge – ioT framework and prototype based on blockchain for smart healthcare applications. *Eng Tech Applied Sci Res*. 2021;11(4):7326–7331. doi:10.48084/etasr.4245
38. Alshathri S, El-Sayed A, El-Shafai W, Hemdan EE. An efficient intrusion detection framework for industrial internet of things security. *Comput Syst Sci Eng*. 2023;46(1):819–834. doi:10.32604/csse.2023.034095
39. Aljuhani A IDS-Chain: a collaborative intrusion detection framework empowered blockchain for internet of medical things. In: 2022 IEEE Cloud Summit, New York: IEEE; 2022: 57–62. doi:10.1109/CloudSummit54781.2022.00015.
40. Akram F, Li D, Zhao P, Kryvinska N, Abbas S, Rizwan M. Trustworthy intrusion detection in E-Healthcare systems. *Front Public Health*. 2021;9. doi:10.3389/fpubh.2021.788347
41. Bassene A, Gueye B. DeepDDoS: a deep-learning model for detecting software defined Healthcare IoT networks attacks. In: *Ubiquitous Networking*. Berlin: Springer;2021:201–209. doi:10.1007/978-3-030-86356-2_17
42. Jain A, Singh T, Sharma SK. Security as a solution: an intrusion detection system using a neural network for IoT enabled healthcare ecosystem. *Interdisc J Info Knowledge Manage*. 2021;16:331–369. doi:10.28945/4838
43. Tahir B, Jolfaei A, Tariq M A novel experience-driven and federated intelligent threat-defense framework in IOMT. IEEE Journal of Biomedical and Health Informatics. January 2024:1–8. doi:10.1109/jbhi.2023.3236072.
44. Haque NI, Rahman MA. PHASE: Security ANALYZER FOR NEXT-GENERATION SMART PERSONALIZED SMART HEALTHCARE SYSTEM. In: 2022 IEEE International Conference on Digital Health. New York: IEEE; 2022:208–214. doi:10.1109/ICDH55609.2022.00040.
45. Alsemmeari RA, Dahab MY, Alsulami AA, Alturki B, Algarni S. Resilient Security Framework using TNN and blockchain for IOMT. *Electronics*. 2023;12(10):2252. doi:10.3390/electronics12102252
46. Zhang G, Liu Y, Bao X, et al. TSDroid: A novel android malware detection framework based on temporal & spatial metrics in IoMT. *ACM Trans. Sens. Netw.* 2023;19(3):1–23. doi:10.1145/3532091
47. Vijayalakshmi P, Karthika D. Hybrid dual-channel convolution neural network (DCCNN) with spider monkey optimization (SMO) for cyber security threats detection in internet of things. measurement. *Sensors*. 2023;27:100783. doi:10.1016/j.measen.2023.100783
48. Cai X, Zhang Z, Zhang Z, Zhang W, Chen J. MODSC: Many-objective-optimization-driven data-balancing strategy in cross-architectural malware classification for Extreme IoT. *IEEE Int Things J*. 2024;11(3):3702–3710. doi:10.1109/jiot.2023.3309337
49. Haque NI, Khalil AA, Rahman MA, Amini M, Ahamed SI. BIOCAD: Bio-inspired optimization for classification and anomaly detection in digital healthcare systems. In: 2021 IEEE International Conference on Digital Health. New York: IEEE; 2021:48–58. doi:10.1109/ICDH52753.2021.00017.
50. Haque NI, Rahman MA, Ahamed SI. DeepCAD: A stand-alone deep neural network-based framework for classification and anomaly detection in smart healthcare systems. In: 2022 IEEE International Conference on Digital Health. New York: IEEE; 2022:218–227. doi:10.1109/ICDH55609.2022.00042.
51. Kumar A, Sharma I Augmenting IoT healthcare security and reliability with early detection of iot botnet attacks. In: 2023 4th International Conference for Emerging Technology. New York: IEEE; 2023. doi:10.1109/INCET57972.2023.10170738.
52. Kumar A, Sharma I Enhancing data privacy of iot healthcare with keylogger attack mitigation. In: 2023 4th International Conference for Emerging Technology. New York: IEEE; 2023. doi:10.1109/INCET57972.2023.10170531.
53. Saritha K, Sarasvathi V, Singh A, Aparna R, Saxena H, Sai Shruthi S Detection and mitigation of man-in-the-middle attack in iot through alternate routing. In: Proceedings - 6th International Conference on Computing Methodologies and Communication. New York: IEEE; 2022:341–345. doi:10.1109/ICCMC53470.2022.9753832.
54. Kalapaaking AP, Khalil I, Yi X. Blockchain-based federated learning with SMPC model verification against poisoning attack for healthcare systems. *IEEE Trans Emerging Top Comput*. 2023;1–11. doi:10.1109/tetc.2023.3268186
55. Tariq U, Ullah I, Uddin MY, Kwon SJ. An effective self-configurable ransomware prevention technique for IOMT. *Sensors*. 2022;22(21):8516. doi:10.3390/s22218516
56. Rughoobur P, Nagowah L A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare. In: 2017 International Conference on Infocom Technologies and Unmanned Systems: Trends and Future Directions. New York: IEEE; 2018:811–817. doi:10.1109/ICTUS.2017.8286118.
57. Ali SE, Tariq N, Khan FA, Ashraf M, Abdul W, Saleem K. BFT-IOMT: A blockchain-based trust mechanism to mitigate SyBiL attack using fuzzy logic in the internet of medical things. *Sensors*. 2023;23(9):4265. doi:10.3390/s23094265
58. Kamel SOM, Elhamayed SA. Mitigating the impact of iot routing attacks on power consumption in IoT healthcare environment using convolutional neural network. *Int J Comput Network Inf Secur.* 2020;12(4):11–29. doi:10.5815/ijcnis.2020.04.02
59. Wang L, Ali Y, Nazir S, Niazi M. ISA evaluation framework for security of internet of health things system using AHP-TOPSIS methods. *IEEE Access*. 2020;8:152316–152332. doi:10.1109/access.2020.3017221
60. Lally G, Sgandurra D. Towards a framework for testing the security of iot devices consistently. In: *Emerging Technologies for Authorization and Authentication*. Cham: Springer;2018:88–102. doi:10.1007/978-3-030-04372-8_8
61. Alsubaei FS, Abuhussein A, Shandilya V, Shiva SG. IOMT-SAF: Internet of medical things security assessment framework. *Internet Things*. 2019;8:100123. doi:10.1016/j.iot.2019.100123
62. Opara HJ, Hill T, Chung L. A framework for representing internet of things security and privacy policies and detecting potential problems. In: *37th Annual ACM Symposium on Applied Computing*. New York: ACM;2022:198–201. doi:10.1145/3477314.3508385
63. Kammuller F combining secure system design with risk assessment for IoT healthcare systems. In: 2019 IEEE International Conference on Pervasive Computing and Communications Workshops. New York: IEEE; 2019:961–966. doi:10.1109/percomw.2019.8730776.
64. Zakaria H, Bakar NAA, Hassan NH, Yaacob SE. IoT security risk management model for secured practice in healthcare environment. *Procedia Comput Sci*. 2019;161:1241–1248. doi:10.1016/j.procs.2019.11.238
65. Salih FI, Bakar NAA, Hassan NH, Yahya F, Kama N, Shah J. IoT security risk management model for healthcare industry. *Malaysian J Comp Sci*. 2019;131–144. doi:10.22452/mjcs.sp2019no3.9
66. Qahtan S, Yatim K, Zaidan AA, et al. Novel multi security and privacy benchmarking framework for blockchain-based iot healthcare industry 4.0 systems. *IEEE Trans Ind Inform*. 2022;18(9):6415–6423. doi:10.1109/tii.2022.3143619

67. Tomashchuk O Threat and risk management framework for eHealth IoT applications. In: ACM International Conference Proceeding Series. New York: ACM; 2020:120–126. doi:10.1145/3382026.3431250.
68. Park SH, Park H. PIER: cyber-resilient risk assessment model for connected and autonomous vehicles. *Wireless Networks*. 2022. doi:10.1007/s11276-022-03084-9
69. Proposal for a regulation - The European Health Data Space - European Commission. 2022. Available from: https://health.ec.europa.eu/publications/proposal-regulation-european-health-data-space_en. Accessed April 07, 2024.
70. Regulation (EU) 2023/2854 of the European parliament and of the council of 13 December 2023 on harmonised rules on fair access to and use of data and amending regulation (EU) 2017/2394 and directive (EU) 2020/1828 Available from: http://data.europa.eu/eli/reg/2023/2854/oj/eng. Accessed April 07, 2024.
71. Biasin E, Yaşar B, Kamenjašević E. New cybersecurity requirements for medical devices in the EU: the forthcoming European health data space, data act, and artificial intelligence act. *Law Tech Humans*. 2023;5(2):43–58. doi:10.5204/lthj.3068
72. EU Data Act's Impact on Medical Devices Data Sharing. 2024. Available from: https://cms-lawnow.com/en/ealerts/2024/01/adapting-to-The-new-eu-data-act-implications-for-medical-devices-and-other-health-devices. Accessed April 07, 2024.
73. Select updates for the premarket cybersecurity guidance: Section 524B of the FD&C Act. 2024. Available from: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/select-updates-premarket-cybersecurity-guidance-section-524b-fdc-act. Accessed April 07, 2024.
74. Chase M, Coley SC, Daldos R, Zuk M Next Steps toward managing legacy medical device cybersecurity risks. Nov. 2023. Available from: https://www.mitre.org/news-insights/publication/next-steps-toward-managing-legacy-medical-device-cybersecurity-risks. Accessed April 07, 2024.
75. P2621 - standards for wireless diabetes device security assurance. 2024. Available from: https://sagroups.ieee.org/2621/. Accessed April 07, 2024.
76. IEEE Medical Device Cybersecurity Certification Program. IEEE Standards Association, 2024. Available from: https://standards.ieee.org/products-programs/icap/programs/medical-devices-cybersecurity/. Accessed April 07, 2024.
77. Four foundational technology trends to watch In 2024. IEEE Standards Association, 2024. Available from: https://standards.ieee.org/beyond-standards/2024-foundational-technology-trends/. Accessed April 06, 2024.
78. Medical devices: council endorses new measures to help prevent shortages. 2024. Available from: https://www.consilium.europa.eu/cs/press/press-releases/2024/02/21/medical-devices-council-endorses-new-measures-to-help-prevent-shortages/. Accessed April 07, 2024.
79. UDI/Devices registration - European Commission. 2017. Available from: https://health.ec.europa.eu/medical-devices-eudamed/udidevices-registration_en. Accessed April 07, 2024.
80. Khan AA, Wagan AA, Laghari AA, Gilal AR, Aziz IA, Talpur BA. BIOMT: a State-of-The-Art consortium serverless network architecture for healthcare system using blockchain smart contracts. *IEEE Access*. 2022;10:78887–78898. doi:10.1109/access.2022.3194195