Information Fusion 102 (2024) 102060

Contents lists available at ScienceDirect

Information Fusion

journal homepage: www.elsevier.com/locate/inffus

Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions

Shams Forruque Ahmed [a,*], Md. Sakib Bin Alam [b], Shaila Afrin [a], Sabiha Jannat Rafa [a], Nazifa Rafa [c], Amir H. Gandomi [d,e,*]

[a] Science and Math Program, Asian University for Women, Chattogram 4000, Bangladesh
[b] Data Science and Artificial Intelligence, Asian Institute of Technology, Chang Wat Pathum Thani 12120, Thailand
[c] Department of Geography, University of Cambridge, Downing Place, Cambridge, CB2 3EN, UK
[d] Faculty of Engineering & Information Technology, University of Technology Sydney, Sydney, NSW, 2007, Australia
[e] University Research and Innovation Center (EKIK), Óbuda University, 1034 Budapest, Hungary

ARTICLE INFO

Keywords:
IoMT
Internet of medical things
Data fusion
Smart healthcare
IoT
Internet of Things
Blockchain

ABSTRACT

The Internet of Medical Things (IoMT) has created a wide range of opportunities for knowledge exchange in numerous industries. The opportunities include patient empowerment, healthcare collaboration, medical education and training, remote monitoring and telemedicine, customized treatment plans, data sharing for innovation, continuous medical learning, supply chain management, public health initiatives, wearable health devices, and quality improvement initiatives. However, the adoption of IoMT faces numerous challenges regarding interoperability, data privacy, security, regulatory, and infrastructure costs. This paper aims to address the implications of data fusion in IoMT, as well as the associated security challenges and their potential solutions, which are lacking in the literature. Data collected from IoMT devices has a direct impact on the accuracy of predictions because of its quality, quantity, and relevance. With an accuracy of 99.53 % to 99.99 %, the Epilepsy seizure detector-based Naive Bayes (ESDNB) algorithm is found to be the most effective for detecting epileptic seizures in IoMT networks. However, the way data are stored must also undergo a major revolution, and all phases—collection, protection, and storage—need to be improved. The standardization of architecture and security measures may improve the detection of security threats and compromises. Methods to detect malware in cross platforms is also an avenue for future research that can effectively tackle the heterogeneity of the IoMT systems. Cryptography and blockchain technology have shown to be promising ways to increase the security of an IoMT-based system. The findings of this review will assist a wide variety of stakeholders in the healthcare ecosystem.

1. Introduction

Current healthcare practices employ manual administration and maintenance of patient data, drug stock, case histories, billing, diagnoses, and medications, which can run the risk of significant human errors that can affect patients. The healthcare system is supported by a network of centralized agents that freely exchange raw data [1]. Internet of Things (IoT)-based healthcare eliminates human error by connecting all devices that monitor vital signs to a decision support system via a network, thereby aiding physicians in making more accurate and timely diagnoses [2]. Thus, IoT is poised to emerge as a major technological advancement of our time [3]. As a result of the numerous potential uses that IoT offers, it is expected to grow significantly and reach more than 24.1 billion devices globally in 2030, an equivalent of almost four devices per person [4]. As IoT technology has been rapidly adopted by the medical industry, the Internet of Medical Things (IoMT), which collects, processes, and analyzes the medical data produced by an extensive number of IoT devices, has also advanced rapidly [5]. IoMT is a network of connected medical devices that transfer data through the cloud [6]. These devices can share and collect data using a variety of standards and technologies since they are connected and interconnected [7]. As a result, IoMT has decreased hospital visits and is seen as a remedy for the shortage of medical resources [8]. Thus, IoMT can successfully increase disease treatment efficiency and accessibility, decrease errors, enhance patients' experiences, and minimize costs [9]. The global IoMT market is

* Corresponding authors.
E-mail addresses: shams.ahmed@auw.edu.bd, shams.f.ahmed@gmail.com (S.F. Ahmed), gandomi@uts.edu.au (A.H. Gandomi).

https://doi.org/10.1016/j.inffus.2023.102060
Received 6 June 2023; Received in revised form 6 September 2023; Accepted 28 September 2023
Available online 29 September 2023

Acronyms

AAMI	advancement of medical instrumentation
ABE	attribute-based encryption
ACL	access control list
AI	artificial intelligence
BGL	blood glucose level
BGL	blood glucose level
CNN	convolutional neural network
DBP	diastolic blood pressure
DNN	deep neural network
DoS	denial-of-service
DTMC	discrete-time Markov chain
ECG	electrocardiogram
ECNN	enhanced convolutional neural network
EEG	electroencephalogram
ESD	epilepsy seizure detector
ESDNB	epilepsy seizure detector based Naive Bayes
FRA	Fletcher reeves algorithm
GDPR	general data protection regulation
GPRS	general packet radio service
H2B	heartbeats-2-Bits
ICD	implantable cardioverter-defibrillators
ICU	intensive care unit
iDDS	integrated drug delivery system
IFTTT	if this then that
IMD	implantable medical device
IoMT	Internet of Medical Things
IoT	Internet of Things
IWD	internet of wearable device
LSTM	long short-term memory
MDLSTM	modified deep long short-term memory
MEmoR	multimodal emotion recognition
MitM	man-in-the-middle
ML	machine learning
MRI	magnetic resonance imaging
PCTL	probabilistic computational tree logic
PD	Parkinson's disease
PET	positron emission tomography
PPG	photoplethysmographs
PSPH	premium seizure prediction horizon
PTP	phase transition predictor
PTT	pulse transit temporal
RBAC	role-based access control
RCC	remote clinical consultation
RFID	radio frequency identification
RSK	randomly-generated symmetric key
SBP	systolic blood pressure
SHS	smart healthcare surveillance
SNR	signal-to-noise ratio
SoC	strength of crowd
SVM	support vector machine
TLS	transport layer security
UAM	user activity model
VPN	virtual private network
WSN	wireless sensor networks
XGBoosting	extreme gradient boosting

estimated to expand from $72.5 billion in 2020 to $188.2 billion in 2025, with the largest compound annual growth rate anticipated in Asia Pacific as a result of policies that support globalization [10].

The initial stage for intelligent services to utilize IoMT is to perceive and collect data about environments and physical items. The employment of many sensors is required to raise the depth of the data fusion outcome and to broaden the range of information received, as a single sensing modality often proves to be insufficient [11]. However, distributing all of the data would be inefficient in terms of network bandwidth and device power due to the heterogeneity of the several sources and volume of sensory data. In order to increase data quality and facilitate decision-making, data fusion becomes an important technique to extract crucial data from widely sensed or gathered data. Data fusion is the study of efficient methods to transform data collected at different times and from different locations into a unified representation that can be used to make decisions, either by humans or machines. Data fusion has several specific applications, including optimization of data quantity, reduction of data size and dimension, and information extraction from data [11]. It assists in removing data anomalies and defeats the collusion of detected data from several sensors. There is abundant sensitive patient information in the heterogeneous data generated by the data fusion process, which is at risk because neither the collecting terminal nor the processing center can be trusted [12].

The disclosure of sensitive data may be caused by both active and passive attacks. Due to their careless deployment into networks, IoMT devices are more susceptible to hackers than those in any other sector. Cyberattacks can affect nearly 50 % of all IoMT equipment [9,10]. A new privacy-aware framework that effectively detects attacks while still protecting users' privacy on multiple levels was proposed by Al-Hawawreh & Hossain [13]. The proposed method stored and distributed the gathered IoMT data among several cloud nodes and encrypted the more sensitive parts. A smart data fusion module was also introduced to efficiently combine IoMT from multiple sources and protect user privacy. The proposed framework also used a differentially private contractive deep autoencoder. With an overall accuracy and detection rate of 99 %, the proposed framework outperformed existing IoMT attack detection models while also protecting the privacy of the collected data. Systems like IoMT stand apart from others because they can affect the lives of patients and raise privacy concerns if patients' identities are made public. Additionally, the average cost of compromising healthcare data is 50 times greater than leaking credit card information [9]. As a result, one of the key prerequisites for a robust IoMT system success is security. IoMT systems that deal with healthcare data should exercise diligence at all times, especially when collecting, transmitting, and storing data.

Due to the market's inherent vendor competition, IoMT products need to develop quickly. As a result, non-standard devices with disparate data transfer standards and heterogeneous communication protocols are created, which leads to security, privacy, and authentication problems [14,15]. The weaknesses inherent in the IoMT infrastructure are often exploited by adversaries as a launching pad for various attacks. Due to the critical nature of security concerns in the IoMT realm, previous review studies have predominantly focused on identifying security challenges and proposing strategies to mitigate risks associated with IoMT products. However, the exploration of the implications of data fusion within the IoMT domain remains largely unexplored. Table 1 highlights and compares the topics covered in recent review works on IoMT in relation to the subject matter of this paper.

The objectives of this review were established based on the identified research gaps and the following research questions:

(i) In the context of the IoMT, what are the most important data fusion techniques utilized to combine data from various medical sensors and devices?

Table 1
Comparative analyses of the topics covered in this review study with some of the recently published review studies.

Study	Primary objective	Architecture	Data fusion	Security issues	Solutions to security issues
This study	Explores the importance of data fusion in IoMT and associated security challenges and mitigation strategies to shed light on IoMT.	√	√	√	√
[16]	Identifies vulnerabilities in currently available medical equipment, along with potential solutions and regulatory measures.	√	×	√	√
[17]	Reviews state-of-the-art IoT-based sensors and sensor systems for taxonomic representation, including privacy and security issues associated with sensor data and methods to resolve them.	×	×	√	√
[18]	Discusses the applications, technologies and architecture of IoMT, and security improvements that occurred to tackle COVID-19.	√	×	√	√
[9]	Reviews existing techniques to improve the security of IoMT systems' data during collection, transmission, and storage by providing a comprehensive overview of potential attacks.	√	×	√	√
[19]	Discusses the benefits of IoMT applications in healthcare; provides an insight into technologies that complement IoMT as well as the difficulties with establishing a "smart" healthcare system.	√	×	√ (brief)	×
[20]	Highlights the architecture and use of IoMT technology in the healthcare system.	√	×	√ (brief)	×
[21]	Provides a categorization of security threats as well as security counter-measures.	√	×	√	√
[22]	Analyzes the many digital system architectures already in-use in healthcare, including their approaches, limits, and the present challenges facing the e-health sector.	√ (brief)	×	√	√
[23]	Systematically reviews articles published during COVID-19 by designing a taxonomy for the categorization of various aspects of IoMT.	√	×	√ (brief)	×
[24]	Comprehensively reviews IoMT and its architecture, discusses the obstacles and potential solutions, and suggests future guidelines for the use and implementation of IoMT.	√	×	√	√
[4]	Investigates the role of machine learning-based intrusion detection systems in resolving security and privacy concerns in IoMT infrastructures.	√	×	√	√
[25]	Analyses in-depth the security concerns associated with IoMT (and IoT).	√	×	√	√
[26]	Describes why certain security strategies, requirements, and design obstacles are essential, and how to overcome them.		×	√	√

√ available; × not available.

(ii) How does data fusion in the IoMT contribute to the development of useful knowledge and the enhancement of healthcare outcomes?
(iii) How is the IoMT different from conventional healthcare IT systems, and what are the most pressing security concerns?
(iv) When it comes to patient privacy and safety, what may happen if there were a security breach in the IoMT?
(v) When it comes to protecting information in the IoMT, what role do cryptography, authentication, and other forms of access control play?
(vi) To what extent may artificial intelligence and machine learning be used to identify and counteract security risks in the IoMT?
(vii) How are issues of data privacy and security in the IoMT currently being addressed, and what are the regulatory and legal considerations involved?
(viii) When collecting and using private medical information, what are the potential ethical implications and issues that may arise?

Based on the identified research gaps and research questions, the present paper investigates IoMT architecture, data fusion on IoMT, and security issues with IoMT and their potential solutions. Notably, this paper distinguishes itself by incorporating valuable insights into the impact of data fusion on IoMT. It commences by introducing the most prevalent types of IoMT currently in use, as well as an overview of the general IoMT architecture. The implications of data fusion in the context of IoMT are highlighted. The paper also thoroughly explores and presents potential solutions to the persisting security issues encountered in IoMT.

The findings of this review will assist with advances in healthcare technology and practices, thereby benefiting a variety of people as well as communities. For instance, researchers can gain access to useful information for medical advances and learning resources, while healthcare providers may reduce errors, streamline workflows, and improve patient care. Insights provided in the study can also help policymakers and healthcare administrators lower expenses, make valuable policies, and better allocate resources. There is also potential for growth and improvement in the health technology industry.

The present paper is organized as follows: Methodological approaches implemented to collect, organize, and analyze relevant data for this review are thoroughly discussed in Section 2. Different types of IoMT are introduced and described in Section 3. Section 4 explores and analyzes the architectures employed in the IoMT. Data fusion in IoMT is explored in various contexts, and the results are summarized in Section 5. The security issues that arise with IoMT and their potential solutions are explored in Section 6. Open issues and current challenges are summarized in Section 7. Section 8 outlines the potential future research in order to minimize the identified challenges in IoMT. Finally, Section 9 provides a concluding review of the study, wherein the key points are summarized and emphasized.

2. Methodology for collecting, organizing, and analyzing relevant data

This review study aims to shed light on IoMT, its applications, and the associated security issues and solutions using an integrative literature method, including comprehensive collection, careful filtering, and thorough evaluation of relevant and high-quality papers. Searches were conducted using databases from well-known sources like Google Scholar and Scopus, as well as the journals of esteemed publishers like Nature, Elsevier, De Gruyter, Taylor & Francis, Wiley, Springer, Inderscience, IEEE, ACM, and Sage. Publications were searched using the keywords "IoMT", "Internet of medical things", "Data fusion", "Smart healthcare", "IoT", and "Internet of Things" to find those most relevant to this study. After that, the extra relevant papers were uncovered by filtering and collecting the aforementioned publications' bibliographies and references. The following criteria were used to thoroughly examine the abstract, introduction, and conclusion of these chosen papers, and a final classification was arrived at:

(i) Concentrating mostly on peer-reviewed works from the aforementioned reputable websites and publishers;
(ii) Accumulating published works of working researchers in the field;
(iii) Including an appropriate balance of both new and older studies;

(iv) Including references to relevant commercial sites where the aforementioned search terms can be found, as well as references to cutting-edge technology that are relevant to the present research;

(v) Returning to the original sources and retrieving critical papers that were referenced in subsequent research, reviewing the prior literature revealed several uncertainties about this report that required additional research to explain the issues at hand and strengthen the overall quality of the investigation. Some keywords were carefully maintained to follow the thought process and investigate the necessary publications to guarantee the necessity of the logical aspect of examining the literature in this study. When brainstorming this paper's topic, the terms "IoMT", "Internet of Medical Things", "Data fusion", "Smart healthcare", "IoT", and "Internet of Things" came to the top. It is essential to have the criteria aiming to limit and filter the scope, as it is thought that relevant publications have much larger importance than the literature volume. Table 2 outlines the inclusion and exclusion criteria used to choose the papers that formed the basis of this study.

Despite being a part of the selection and limiting process for the literature, the criteria for exclusion seemed quite judgmental. For this reason, the authors implemented a test-retest procedure, in which the retrieved data are checked for accuracy a second and even third time following a random choice from primary research. To help readers comprehend the primary material of this study, a holistic overview based on pre-exploratory mapping is shown in Fig. 1a. Using the existing publication categorization system, a comprehensive outline was developed. In the end, 1372 publications were collected for analysis, but only 137 were included in this review paper, as seen in the chronological distribution of publications in Fig. 1b.

3. Types of IoMT

IoMT systems can help cure numerous medical diseases by providing an effective pathway for better diagnoses and treatments. By enhancing work efficiency, enabling remote monitoring and diagnostics, and improving patient care, IoMT has the potential to completely transform the healthcare industry. For instance, some medical issues necessitate the use of implantable devices like pacemakers to ensure that the heart continues to beat normally [28]. Other devices that are wearables, like smartwatches, provide a better, noninvasive healthcare experience to monitor different organs of the body [29]. Due to these distinctions, the IoMT systems can be divided into two groups: implantable medical devices (IMDs) and Internet of Wearable Devices (IWDs). An overview of these types is provided in Table 3.

3.1. Implantable medical devices

Implantable medical devices are gadgets that can be inserted into the body to detect, monitor, and treat diseases. These devices are often implanted by surgical treatment or inserted into the body utilizing minimally invasive techniques. They may perform specific tasks or provide current medical help, depending on the needs of the individuals. For instance, a pacemaker is an IMD that helps with the treatment of irregular heartbeat by stimulating the heart to beat normally when it is beating too quickly or too slowly [30]. Wireless implantable medical devices are important in modern healthcare because they offer a variety of advantages and benefits. By eliminating the need for cables or connections, implantable wireless devices allow patients to move around more easily and comfortably. Therefore, low power consumption, limited storage space, and long lifespan, compact batteries are crucial criteria for these devices to stay within a human body for an extended duration. For example, pacemaker implants typically survive between 5 and 15 years [9]. Wireless implanted devices can be equipped with sophisticated safety measures, including automatic notifications and alarms, to alert medical professionals and patients of any serious accidents or irregularities. Rapid medical attention and response, therefore,

Table 2
Criteria for identifying appropriate literature [27].

Inclusion guidelines	Exclusion guidelines
- Publications chosen for this research must be scientific and peer-reviewed and must be both relevant and capable of answering the research questions. - Gray literature is also thoroughly researched because of its potential usefulness and importance.	- Even if they were scholarly and peer-reviewed, publications that omitted or inadequately discussed the information relevant to the aforementioned keywords would be disqualified. - Gray literature with redundant findings or lacking appropriate references or contexts will be excluded. In addition, the current analysis only considered conference proceedings to a limited extent.

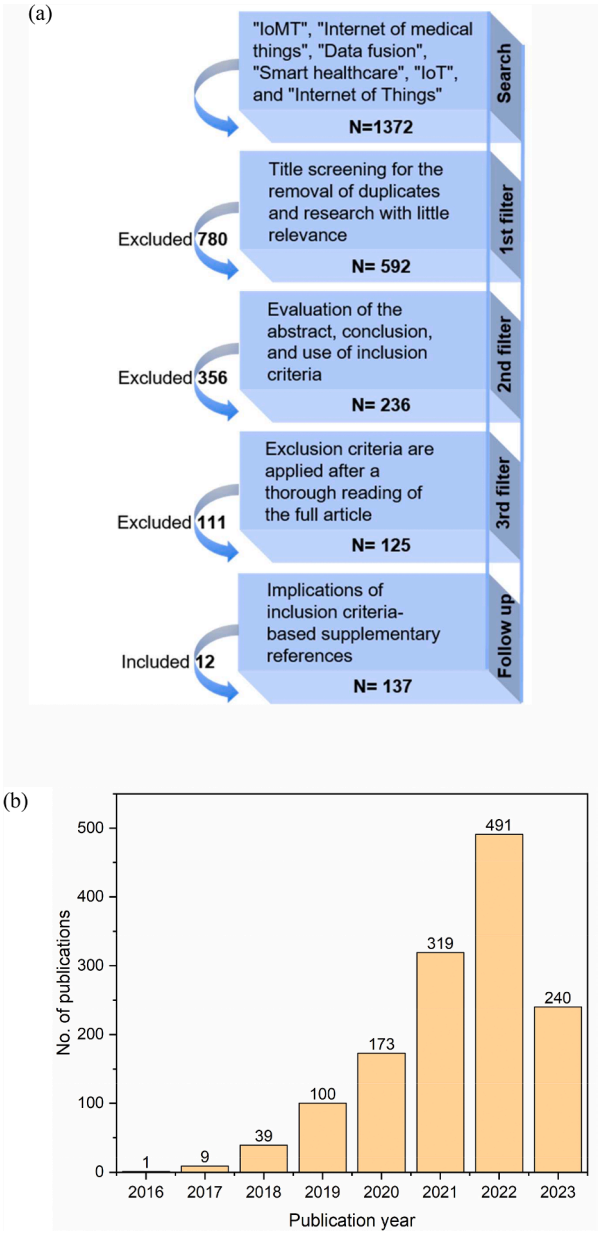

Fig. 1. (a) Literature selection and filtering process flowchart, where N is the number of publications; (b) yearly publication distribution since 2010.

Table 3
Overview of the types of IoMT.

IoMT type	Devices	Main Task	Outcome	Advantages	Disadvantages	Ref.
Implantable medical devices	Pacemaker	Cardiac resynchronization treatment; immediate communication between Bluetooth low-energy pacemaker devices.	Successful transmission percentage of 92.8 %, which is higher than that of prior console-based remote monitoring systems, and a success rate of 94.6 %.	Enhanced transmission is accomplished through less patient burden, higher automaticity, selective initiation, and user-friendly systems.	The controls for enforcing the arrangement of transmissions and survey completions were limited.	Tarakji et al. [32]
	Seizure predictor	Accurately forecast epileptic seizures in real time before they commence	The model produced an accuracy of 97 % and a precision of 96.11 %.	Effective seizure prediction for epileptic patients; implementing the appropriate precautions to lessen the effects of these seizures.	The seizure patterns, causes, and characteristics may vary widely between individuals.	Banu et al. [33]
	Seizure detector with drug delivery unit	Real-time seizure detection and administration of the medication to the desired location	Showed 100 % sensitivity and a latency of 1.8 s on average; delivered lower power usage based on simulation results.	The system allowed for a significant decrease in power consumption and an improvement in detection accuracy.	Data security and privacy issues were a concern for this study, especially in the drug delivery system.	Sayeed et al. [34]
	Nanogenerator and cardiac pacemaker	Internal energy conversion from mechanical to electrical; ventricular pumping and monitoring function	Increases in an active area and surface charge density resulted in better electrical output after a few modifications were made to the surface.	Energy harvesting was successfully demonstrated by Bluetooth monitoring of live output voltage data.; capacity of self-recharging a lithium-ion battery.	Device interference and compatibility; for example, a pacemaker might get affected by electromagnetic fields of MRI.	Ryu et al. [40]
Internet of wearable devices	Cardiorespiratory tracker	Cardiac signal processing and data transmission enable the wireless transfer of the collected information	Calculating breathing rate from heart rate using only pulse amplitude.	Simple to use, portable, and smaller in size than other gadgets.	Occasionally might set off misleading alerts identifying unusual heart rates or breathing patterns in terms of no such emergency; these false alarms may trigger tension, anxiety, or medical treatments.	Sasidharan et al. [36]
	Wristwatch	Measuring blood pressure	Surpassed the AAMI standard for the non-automated sphygmomanometer and demonstrated accuracy equivalent to oscillometry-based devices.	CareUp performed well in the estimation of SBP and even superior in the estimation of DBP compared to other devices; the p-values generated by CareUp were consistently higher.	Limited user interface; reduced battery life; data privacy and security concerns.	Lazazzera et al. [37]
	Heartbeats-2-Bits (H2B) (piezo sensor)	Measuring heartbeat intervals at numerous sites of the human body	The pairing has a robust success rate of 95.6 %.	As evident from the power tests, H2B is exceedingly power-efficient.	The strong cardiac signal might be collapsed into physical movements.	Lin et al. [38]
	Smartwatch	Record rest tremors in PD patients and assess their clinical association	The Spearman relationship between the mean resting tremor scores and the tremor intensity readings was 0.81 ($p<0.001$).	Has the ability to export wireless tremor intensity records over time in order to obtain clinically appropriate data.	Low amplitude noise in the signals recorded by the gyroscopes may have an impact on tremor assessment.	Roberto et al. [39]

improve patient outcomes and safety. Wireless connectivity enables medical professionals to remotely set and customize implantable devices according to patients' needs and requirements. Without required invasive procedures or device replacements, individualized treatment regimens and adjustments are available because of this flexibility. Implantable medical devices include pacemakers, implantable cardioverter-defibrillators (ICDs), and neurostimulators [31].

A smartphone application was developed by Tarakji et al. [32] that allows for immediate communication between Bluetooth low-energy pacemaker devices for cardiac resynchronization treatment and smart gadgets. A BlueSync field evaluation was carried out to analyze both patient and healthcare professional input regarding the technology and to measure the efficacy rate of programmed remote monitoring transmissions. It was found that patient-controlled remote monitoring transmissions utilizing an app on their own smartphone or tablet achieved a 94.6 % success rate, which is higher than that of earlier console-based remote monitoring systems when comparing groups by age, gender, and device types. Patients who continued to use the same platform after the evaluation reported an identical transmission success rate of 92.8 %. After one year of treatment, patients reported feeling confident in the procedure's safety and efficacy. These results demonstrate that improved transmission is achieved by reduced patient workload, increased automation, targeted system activation, and simple interfaces. In addition, the use of the app for remote monitoring would positively affect the care of patients with cardiovascular implantable electronic devices by enhancing remote monitoring success and improving patient and provider experiences. However, the study was designed to permit some flexibility in maintaining a conventional clinical practice, so controls for enforcing the arrangement of transmissions and survey completions were limited. Results reveal that 57 % of respondents reported having four scheduled transmissions, while 2.9 % reported having none.

Unpredictable and often prolonged seizures cause the deaths of about 15 % of epileptic patients. Effective seizure prediction that occurs before the onset of the seizure alerts epileptic patients to implement the appropriate precautions to lessen the effects of these seizures, improving their quality of life. Banu et al. [33] created ForeSeiz, a smart, self-cognizant, as well as assertive seizure predictor that is intended to anticipate seizures. The primary objective of this research was to accurately forecast epileptic seizures in real-time before they commence. This architecture was properly designed considering the IoMT foundation. A seizure prediction headband with a total weight of 30 g was

constructed by integrating front-end electronics and a Seizure Predictor Tag. In the proposed ForeSeiz predictor, the Fletcher Reeves Algorithm (FRA) and Phase Transition Predictor (PTP) are incorporated for optimizing an Enhanced Convolutional Neural Network (ECNN) classification model as well as a PTP for predicting the outcome of immediate seizures. Transfer learning was employed to train and evaluate the model on electroencephalogram (EEG) recordings. The model produced a 97 % accuracy, 96.11 % precision, and a Premium Seizure Prediction Horizon (PSPH) of 66.52 min before the initial occurrence of seizures. The Firebase cloud was additionally integrated into the model to record the conditions of epileptic patients. If a seizure is anticipated to start, the caregivers would be notified right away to conduct further intervention measures. However, since the seizure patterns, causes, and characteristics of individuals vary, not all seizures may be predicted.

Around 1 % of the world's population suffers from epilepsy, which highlights the importance of wearable or implantable seizure control devices. For automated seizure identification and management, Sayeed et al. [34] presented an IoMT-based integrated drug delivery system (iDDS) that incorporates a seizure-detecting unit and a medicine distribution unit. A deep neural network (DNN) classifier and statistical feature extraction are also implemented for the real-time detection of seizures. A piezoelectric-operated double reservoir micropump is used to administer the medication to the desired location when the detection process is finished. Results show that the proposed system delivers lower power usage and significantly decreases latency, which is necessary for efficient seizure control. Therefore, this system can be considered a workable instrument for realistic biomedical applications because of its dual reservoir mechanism that increases longevity. It also improved sensitivity while decreasing latency, making it a possible option for use as an implanted low-latency device. However, data security and privacy issue persist as a concern for this study, especially in the drug delivery system that might alter the rate of flow among devices.

3.2. Internet of wearable devices

Wearable devices that monitor vital signs like heart rate have the potential to make a positive impact on people's health. Some common examples include ECG monitors, blood pressure trackers, smartwatches, and fall detection bands [35]. When a user is not moving around, monitoring can be utilized to identify slow and rapid heartbeats. The new watches can also detect breaks and use ECG measurements to diagnose conditions like an irregular pulse. For non-critical patient monitoring, these devices are utilized extensively but cannot likely replace IMDs in life-or-death situations due to sensor accuracy and battery life issues.

A wearable cardiorespiratory tracking device was developed by Sasidharan et al. [36] that can simultaneously record, evaluate, and display four different parameters, including temperature, respiration rate, peripheral capillary oxygen saturation, and heart rate on a mobile phone. The suggested system contains three noncontact sensors that each measure one of the four district metrics in sequence. Numerous cardiovascular, neurological, and even pulmonary conditions may be rapidly and easily identified at an early stage with the aid of continuous monitoring of various physiological markers. The body sensor network of this health monitoring system includes signal processing and data transmission modules, enabling wireless Internet transfer of the collected information. The heart rate of healthy individuals generally ranges between 70 and 80 bpm and stays constant during resting conditions. The range of obtained temperatures was also considered appropriate because it did not go above the normal human body temperature of 37°C. As monitored by the proposed system, the breathing rates, pulse rates, and peripheral capillary oxygen saturations of persons with a history of heart attacks were extremely fluctuated over a week or two. Furthermore, the mobile application stores and evaluates the data collected from individuals, which can be used to help predict the probability of a heart attack and alert users and medical professionals. The proposed system is also simple to use, considering that mobile phones have significantly higher availability and credibility than other electronic devices. The wearable device is more portable and smaller than gadgets that are worn in shirt pockets.

Lazazzera et al. [37] developed the CareUp wristwatch, an innovative wearable device capable of measuring blood pressure in real-time that uses a pulse oximeter on the rear and another oximeter on the front of the watch. The capture of two photoplethysmographs (PPG) is initiated by placing the index finger on the front of the oximeter; then the signals are processed and cross-correlated to obtain a temporal delay between them, defined as the pulse transit temporal (PTT). The systolic and diastolic blood pressure (SBP and DBP, respectively) are then computed using the heart rate information from the finger PPG and PTT measurements. Using a sphygmomanometer, the smartwatch's capability to measure blood pressure was successfully verified. Measurements obtained by CareUp were compared to those of two existing oscillometry-based devices, particularly Thuasne and Magnien, during the evaluation process. The Wilcoxon rank sum analysis was employed in the statistical analysis to compare the standard deviation and mean of the estimate errors. The results nearly surpassed the American Association for the Advancement of Medical Instrumentation (AAMI) standard for non-automated sphygmomanometers and demonstrated accuracy equivalent to oscillometry-based devices. Only DBP was found to be within AAMI's acceptable range, whereas SBP's standard deviation error was two points higher. CareUp performed well in the estimation of SBP and superior in the estimation of DBP compared to the other two devices. The p-values generated by CareUp were consistently higher than those obtained using the other two instruments. However, the model faces a few limitations, including a limited user interface, reduced battery life, and data privacy and security.

Heartbeats-2-Bits (H2B) was developed by Lin et al. [38] for effectively associating wearable devices by creating a shared secret key derived from the skin vibrations generated through the heartbeat. The demand for sophisticated heartbeat monitors like the electrocardiogram was eliminated by detecting heartbeat points efficiently using affordable and energy-efficient piezo sensors, which served as the inspiration for this research. In fact, the trials demonstrated that piezo sensors are capable of measuring heartbeat intervals at numerous body sites, including the chest, waist, neck, and ankle. Since piezo vibration sensors were not intended to be precise heartbeat monitors, it was also found that the heartbeat interval signal they recorded had a low Signal-to-Noise Ratio (SNR). An exponential function-based quantification technique was used to completely derive the accessible entropy from the disruptive piezo readings in order to solve this issue. The H2B was prototyped using well-known piezo sensors, and its performance was assessed using data obtained from various body positions of 23 volunteers. The results demonstrated that H2B had a successful pairing rate of 95.6 %, and its resilience against three distinct types of attacks was also evaluated. Additionally, it was evident from the power tests that H2B is exceedingly power-efficient. However, H2B only succeeded under the present design when a user was performing static actions like sitting, standing, or lying down, which could be due to the sensitivity of piezo sensors to various body motion artifacts. As a result, the strong cardiac signal would be collapsed by the movements. Thus, there is a need for more sophisticated signal processing techniques to solve this issue.

The implementation of wearable technology in Parkinson's disease (PD) research has drawn increasing attention. In order to follow up on PD patients, Roberto et al. [39] proposed a study to examine the viability and dependability of utilizing a system based on smartwatches to record rest tremors in PD patients and to assess their clinical association. The gyroscopes of a smartwatch were utilized to collect raw data for an Android application. A total of 22 PD patients were sequentially enrolled and monitored for a full year. The root mean square of the angular speed recorded by the smartwatch at the wrist serves as the tremor intensity metric. In total, 64 smartwatch evaluations were performed. The

coefficient of reliability with a resting tremor to determine the smartwatch's ability to quantify tremors was 0.89, with a minimum detectable change of approximately 59.03 %. Smartwatches may not pick up vibrations in the proximal fingers because of their location on the wrist. Innovations in finger devices may one day allow us to bypass this restriction. The research also showed that tremor assessment could be affected by low-amplitude noise in the signals acquired by the gyroscopes.

4. IoMT architecture

IoMT provides a secure and efficient platform for collecting, processing, and analyzing medical data to produce useful information and decision-making systems. The architecture of IoMT consists of four essential layers: sensor, edge (gateway/fog), cloud, and interface (Visualization/Action) [41,42], as shown in Fig. 2. Wearable sensors are used to continuously monitor a patient's health problems. The sensor layer remotely collects real-time health-related data from patients through wearable sensors connected to a system, such as Raspberry Pi [41]. The gateway layer performs fuzzification and makes decisions at the edge to generate real-time notifications about a patient's high-risk medical conditions. The cloud layer accumulates the collected data for storage and secure access by authorized personnel for monitoring healthcare and is also accountable for data storage and computing. Security of accessing data is implemented at the action layer using an approval-based method. Moreover, the action layer acts as the direct interface between people and the ecosystem [43]. The gateway layer, which is comprised of local servers and gateway devices, operates between the cloud and action layer. IoMT-based individual health monitoring systems have resolved the issue with traditional health monitoring by allowing sensors on the body to monitor health signals and connect to family and physicians over the Internet [44–46].

4.1. Sensor layer

The sensor layer is the foundation of the IoMT system, which collects data from patients via a variety of sensors and then transmits it to the gateway/cloud for further processing. This layer is made up of hardware, including sensors, controllers, and actuators [47], allowing the accurate detection of the parameters associated with health concerns [48]. The sensor layer is divided into the data-entry and data-processing sublayers [49]. The data process sublayer's main responsibility is data understanding, for which it employs a variety of signal acquisition and medical perception devices. General packet radio service (GPRS), radio frequency identification (RFID), graphic code, and other popular signal acquisition techniques are available [50]. The collected data are subsequently sent to the next state through the data entrance sublayer using short-ranged data transmission techniques, including Bluetooth, Wi-Fi, 4 G, and 5 G [51,52].

Wearable sensors are gaining popularity for numerous applications, including IoMT, because of the precise and trustworthy information they can offer on regular human activities [53]. Wireless and wearable are the two categories of IoMT sensors [54–56]. Wireless cameras and smartphones/smartwatches are the two main categories of wireless sensors [57]. Patients' cognitive signals are captured using wireless cameras like smart video cameras, and the IoMT subsystem is connected to the cloud infrastructure via smartphones and smartwatches with built-in GPS or Bluetooth radios [42]. Besides, wearable gadgets are intelligent sensing devices that can produce data, link to other gadgets, and be worn as fashion accessories. Gestures, temperature, heartbeat, and other signals are all measured by vital sign-measuring devices, such as biosensors [5]. In addition, these devices are primarily utilized by runners and sportsmen to assess blood pressure, respiration rate, electrocardiogram (ECG), and sleep pattern [58,59]. Wearable trackers, like wristwatches and fitness trackers, are wrist-worn gadgets that can detect an individual's bodily activity, such as movement and heartbeat. Furthermore, different types of smart clothing use integrated sensors to

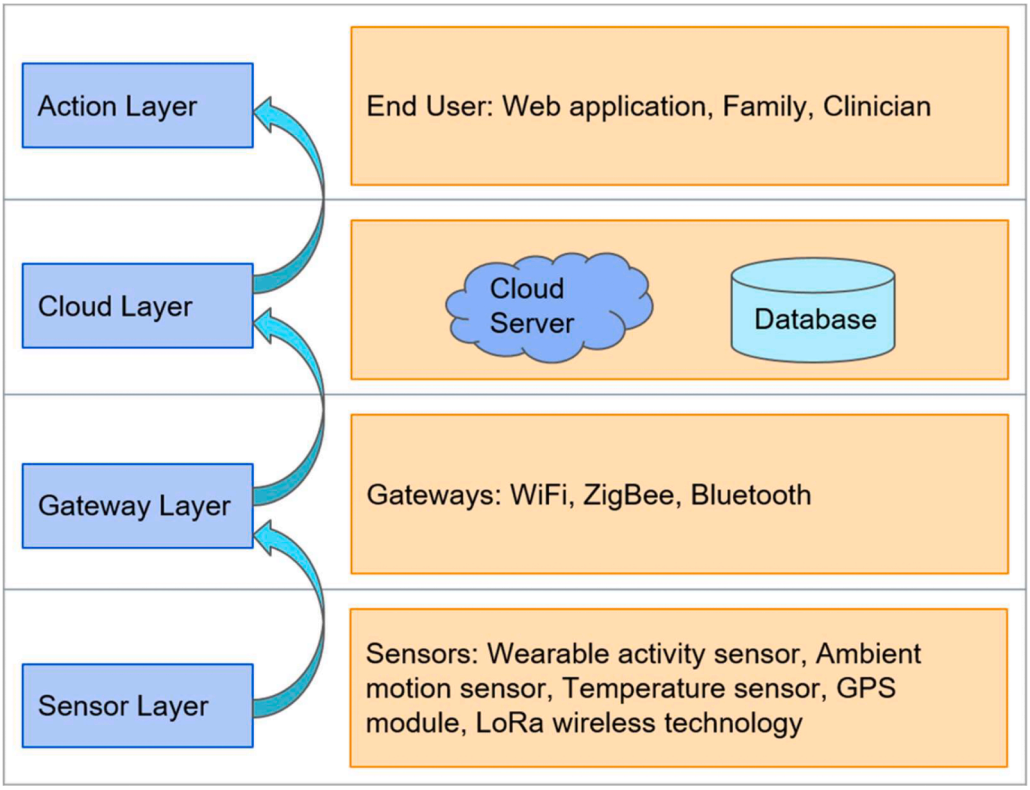

Fig. 2. IoMT architecture.

track various medical problems and collect data that can be pooled and analyzed to offer more thorough health information [60,61].

4.2. Gateway layer

This layer, sometimes referred to as the fog layer or edge layer, comes after the sensor layer and provides a variety of stages, interface-related tasks, and data transfer techniques. This layer is composed of local servers and gateway devices [49], as well as the transmission and service sublayers. Real-time data transfer occurs between the sensor layer and the transmission sublayer. The service layer is used to integrate diverse networks, data warehouses, and data description formats [50]. In edge computing, data preparation is executed in the gateway layer as opposed to the cloud layer. Edge computing offers numerous benefits [62], which may be summed up as follows:

i) The burden on the cloud layer will be lessened since the data are already processed and can be sent from the devices to the cloud layer.
ii) The latency is significantly decreased since the gateway server is close to the IoT devices.
iii) Security and privacy are maintained properly.

The fog layer has been applied in several healthcare applications. Almas et al. [63] suggested a trust solution for smart healthcare systems that is adaptive and dependent on the context, using the principles of fog computing. Many experiments intended to enhance a health monitoring system by utilizing the advanced services available at gateways through fog computation, e.g., distributed data storing, data processing, and notification, which are located at the network's edge. In order to accomplish speed and latency, Farahani et al. [64] offered a patient-focused e-healthcare framework based on cloud and fog layers.

4.3. Cloud layer

The cloud layer has the data storage and computing capabilities required to evaluate the data and develop decision-making applications based on the evaluations [42]. The cloud resources of this layer will store the data generated by the medical devices, allowing for further analytical processing as required. This layer carries out machine learning activities, data warehousing, epidemiological, and statistical medical research. It gives a graphical interface as a finishing touch for feedback and visualization. This cloud architecture allows service providers and caregivers access to epidemics, illness patterns, medical histories, and remote healthcare monitoring [16]. Services like chats, data processing, data storage, and analysis are provided for IoMT systems by cloud platforms, such as Cloud, Microsoft Azure, Amazon Web Services, IBM Cloud, and Google Cloud [65].

Large medical and healthcare systems may easily integrate into the cloud to conduct their daily operations. Noor [62] proposed a technique to identify epileptic seizures by creating a cloud layer to store patient data together with daily updated EEG samples. The required data are subsequently processed and sent to the approved hospitals. A heuristic method, which was introduced by Fouad et al. [66], was used to investigate vertebral tumors. The hospital used a spinal sensor and the transformation software hosted in the cloud to evaluate the acquired data and provide conclusions. Panja et al. [41] utilized a mobile application to retrieve and store the medical information of patients in the cloud. Since acquired medical data are extremely sensitive, a security system that assures the authentication of users was designed to restrict access only to the authorized group of individuals.

4.4. Action layer

The management of medical records is handled by the action/application/visualization layer in IoMT using a variety of applications, including apps, ambient sensors, remote diagnosis, and several non-wearable healthcare devices [47]. The action layer is divided into two sublayers, namely medical information and medical decision-making layers, which are responsible for handling medical information and making decisions, respectively [49]. To maintain patient information, the medical information layer includes a variety of medical tools and information-related materials, tracking systems, remote diagnosis systems, telemedicine, medical e-records, etc. This layer also includes resources linked to medical diagnosis and treatment [47]. Exploration of different information, such as patients, diseases, medications, diagnoses, and treatments, is the focus of the medical data decision-making action layer.

The key roles of the action layer are the interpretation of data and the delivery of application-specific services. To make diagnoses and treatment plans, multiple AI methods, especially deep learning, are employed to analyze the collected data and draw conclusions [19]. Numerous scientific applications are also used in the application layer, including the development of drug activity, gene mutation, diabetes monitoring, heart arrhythmia, and Alzheimer's detection [19]. Overall, the architecture of IoMT systems may differ based on the implementation, the technological choices made, and the healthcare context. The main layers that have been explained above give a general framework that can be used to comprehend the primary components that are involved in the construction of IoMT solutions.

5. Data fusion applications in IoMT

Data fusion techniques are crucial in healthcare as they permit the combination of various data sources to improve clinical practice, medical research, and healthcare decision-making. Data fusion is essential in the IoMT, where many connected devices and data sources revolutionize healthcare. Sensor data fusion is used in IoMT to combine sensor inputs for a complete patient health profile. Feature-level fusion improves patient diagnostics by combining relevant features from multiple sources [67]. Decision-level fusion integrates device and algorithm results to make healthcare decisions holistically. Training models with ML and AI to interpret complex data relationships is used in medical imaging [68]. Temporal and context-aware fusion is essential for disease progression monitoring and environmental health effects. IoMT data fusion is enhanced by ensemble methods, semantic data integration, quality assurance, and privacy-preserving techniques, ensuring data privacy, accuracy, and actionable insights for better patient care and healthcare system efficiency.

Data fusion is used in medical imaging to improve diagnosis and treatment planning for complex conditions by integrating information from several modalities, including positron magnetic resonance imaging (MRI) and emission tomography (PET) computed tomography [69]. Genomic and clinical data fusion integrates genetic and health records to improve diagnosis, treatment, and prognosis [70]. Sensor fusion in remote monitoring also integrates information from mobile apps and wearables for more effective management of chronic conditions and earlier initiation of treatment. These examples demonstrate how data fusion can improve healthcare by providing a more complete picture of patient information and medical research.

IoMT extensively relies on data fusion since it enables the integration and analysis of diverse types of data from multiple sources. The term "IoMT" refers to the grouping of internet-connected medical tools and software that enable data and information sharing. With the IoMT, more data are becoming available from several sources, including clinical systems, wearables, electronic health records, and medical devices. To better diagnose, treat, and manage diseases, data fusion includes combining these many data sources to produce a more complete picture of a patient's health status [5]. By offering intelligent services tailored to gathering and processing data produced by IoT, the cloud IoT, where IoT and cloud mix, has emerged as an enabler to satisfy data fusion qualities [71]. However, data fusion has many uses in IoMT, some of which

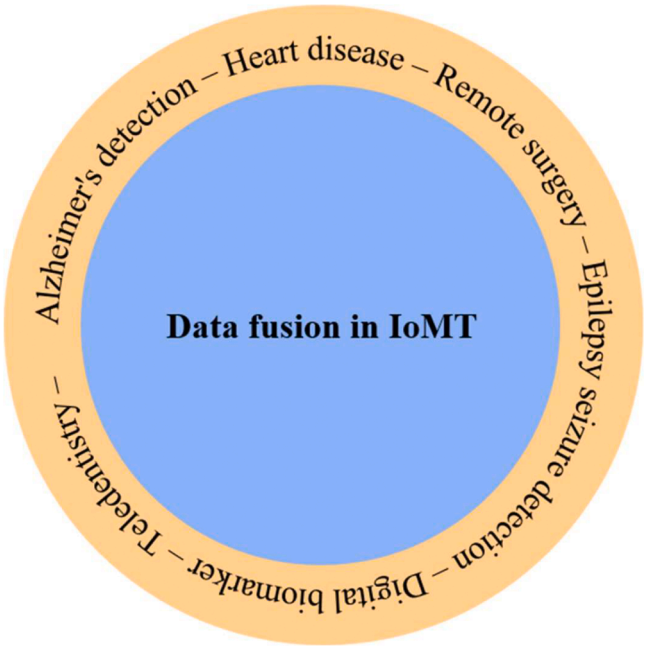

Fig. 3. Applications of data fusion in IoMT.

include: remote surgery, epilepsy seizure detection, digital biomarker, teledentistry, Alzheimer's detection, and heart disease (Fig. 3).

Distributed computing paradigms like mobile-edge computing, transparent computing, and fog computing are replacing centralized computing paradigms in computing models today [72]. By deploying processing resources at the edge nearer to data sources, edge computing and fog computing in this context bring additional features to the cloud and narrow the distance of endpoint IoT gadgets from the cloud [73–75]. The IoT and AI industries are collaborating, and different companies have already included AI in IoT applications. The IoT's full potential could be realized by combining it with AI, which involves machine learning and big data analysis [76].

5.1. Remote surgery

Remote surgery is a cutting-edge surgical technique that connects patients and surgeons who are geographically separated using robotic tools and networking technology. Telesurgery has emerged as a viable alternative for patients in need of urgent and high-quality surgical care, as well as those with a shortage of surgeons and practical restrictions on physician schedules, due to its ability to overcome the limitations of traditional surgery. Yang et al. [77] investigated the use of enhanced 5 G robot-supported laparoscopic surgery in urology. Data from 30 patients who had robot-assisted laparoscopic telesurgery utilizing 5 G technologies were retrospectively examined in this study. According to the research, enhanced robot-assisted laparoscopic telesurgery using 5 G technologies is a practical, secure, and successful method for urological treatments, which can reduce operating room time and blood loss and increase surgical accuracy and precision. The limited sample size and retrospective design of this study, however, are some of its drawbacks.

An intensive care unit (ICU) teleultrasound diagnostic system was proposed by Duan et al. [78]. On the patient's end, there is an ultrasound instrument that is aided by a robotic arm called MGIUSR3, and on the doctor's end, there is a control unit. Both the surgeon's and patient's end include audio, video, and mainframe systems. The kidneys, gallbladders, spleens, livers, and pancreas of 32 patients were imaged using ultrasound technology. Because of intestinal gases and poor image quality, one subject was eliminated from the study. The experiment was successful for the remaining patients, and high-quality images were obtained.

5.2. Epilepsy seizure detection

The prevalence of impulsive seizures—a prominent paroxysmal neurological disorder that is infrequently observed in medicine—is often recognized as epilepsy. In the IoMT, automatic epileptic seizure identification from EEG signals is considered an efficient diagnosis. The EEG signals of various patients are gathered from different locations to a central server to create a reliable detection system in the IoMT architecture. Ding et al. [79] introduced Fed-ESD, a privacy-preserving federated learning architecture that uses fog nodes to facilitate the exchange of location-oriented EEG data for the automatic detection of epileptic seizures. The proposed architecture employs a spatiotemporal transformer architecture to gain spatial and temporal presentations from each participant's data. The study demonstrated that the proposed framework for deployment in IoMT was effective in terms of scalability, detection, and resource efficiency. However, the study lacks the interpretability of epileptic seizure detection decisions. To produce visual or verbal justifications for the detection decisions, explainable AI may be a promising path.

Idress et al. [80] proposed a method to detect epileptic seizures when EEG data is being compressed without loss. The method has three purposes: (i) reduces the amount of EEG data transferred to the cloud; (ii) detects patients who are having epileptic seizures at the fog gateway using the Naive Bayes algorithm; and (iii) compresses data by merging k-means clustering and Huffman encoding from the edge to the fog gateway. The compression capacity was four times that of previous methods, and the accuracy ranged from 99.53 to 99.99 %. Latency rates were reduced from 84.6 % to 88.2 % using the KCHE compared to the non-compressed EEG data method for several different types of EEG data recordings. This will enable the medical team to decide quickly on their patients.

In order to gather information on heart rate, body temperature, muscular spasms, and falls, Hassan et al. [81] developed a monitoring system for Grand Mal Epilepsy Tonic-Clonic seizures employing a variety of sensors, including ECG, EMG, accelerometer, and Dallas sensor. In this system, data are categorized into several seizure kinds using a fuzzy logic algorithm, and the classifications are shown graphically on an IoT dashboard. Using the "If This Then That" (IFTTT) technology, abnormal situations are recognized, and an SMS message is delivered to medical staff. For body temperature, observing heart rate, muscular spasm, and fall identification, the system showed average accuracies of 98.90 %, 95.49 %, 83.0 %, and 87.21 %, respectively. Clustering analysis might be utilized to better categorize and tailor a patient's symptoms.

5.3. Digital biomarker

Finding particular data signatures, also known as digital biomarkers, that may be utilized for categorization or estimating the severity of the underlying conditions is one of the important components of wearable devices with machine learning (ML) techniques. Ahmed et al. [82] described how non-invasive wearable devices may be used to measure blood glucose levels (BGL) in diabetic patients using AI-based methodologies. Glycemic events may be tracked using digital biomarkers, which is a significant advancement in self-monitoring technology. The study examined the effectiveness of AI techniques in calculating BGL among diabetes patients utilizing non-invasive wearable device data. High accuracy was achieved when estimating the link between glycemic measures and characteristics, but the study's limited sample size of only 13 people was a major limitation.

Identifying human emotions in real-time is possible by utilizing data from the Emotional IoT and a deep learning model called MEmoR, as suggested by Kumar et al. [83]. MEmoR employs visual and psychophysiological data as its two data modalities. Video signals are used to record the visual information, and a ResNet50 model that had already been trained is adjusted for emotion categorization. Using a convolutional neural network (CNN), the psychophysiological data are

analyzed. The results from both approaches are integrated by utilizing decision-level weighted fusion. MEmoR achieved accuracies of 83.79 and 81.54 % on the Bio Vid Emo DB multimodal dataset. However, the study did not report how individuals might behave in a changing environment for real-time emotion detection model creation.

A novel approach for diagnosing depression that combines the LSTM and SVM algorithms was presented by Arora et al. [84]. Statistical characteristics are integrated with the features extracted from activity measures using the LSTM. The merged feature map was implemented to train the SVM model, and the Depression dataset was used to test its accuracy, which was 95.57 %. Depression was reportedly assessed using overlapping sliding windows on recordings of motor activity and a mix of statistics and deep learning-derived variables. Future research can include transfer learning models and other behavioral health facets to suggest a paradigm for behavioral health.

5.4. Teledentistry

Comprehensive oral healthcare requires the utilization of patient-centered care, but there are obstacles, such as high treatment costs, an aging population, chronic dental disorders, and difficulties reaching patients in distant places [85]. Telemedicine has been developed as a means of lowering the frequency of dental visits, enabling at-home self-care, and assisting in the identification of various oral disorders. Additionally, telemedicine may bridge the gap in dental treatment discrepancies between urban and rural locations and can monitor patients' health problems.

In order to prevent and identify dental caries in its early stages, Salagare and Prasad [86] presented a creative approach that is built on the IoMT and teledentistry. This technologically-based model offers information on how to manage the oral cavity's caries-causing variables, such as biofilm pH, biofilm presence, and oral cavity temperature, using intraoral sensors attached to appliances. This information is continuously gathered from a patient's mouth cavity and sent to a server via a mobile app. The Internet of Dental Things, artificial intelligence, and telemedicine are used to analyze data. The method is easy to apply at the community level.

In a study by Martin et al. [87], remote clinical consultations (RCCs) were compared to in-person consultations to determine which is more effective for restorative dentistry. A verification consultation took place in-person after 23 patients had RCC performed remotely using high-speed internet and audiovisual transmission. Results demonstrated that RCC was as efficient and secure as in-person consultations, regardless of the user's gender or age. The research intervention team and patients' responses to a theme questionnaire revealed that the GDP, nurse, and patient all made successful contributions to the RCC process. This study, however, did not evaluate the intervention's cost-effectiveness, efficacy under all clinical conditions, or GDPs' acceptability in a real primary care practice.

5.5. Alzheimer's detection

Patients with Alzheimer's disease are typically monitored using wireless sensor networks (WSNs). These patients may experience substantial memory loss, and the independence and well-being of the patients may be impacted by this cognitive impairment. WSN may gather patient activities, for instance, their postures and states, to assist health studies as the fundamental framework for future healthcare systems. To automate the detection of early-stage Alzheimer's disease and early identification of cognitive damage, Yin et al. [88] proposed an IoT architecture employing an eye-tracker (ET) and cloud-based diagnostics made possible by ML. The method uses multimodal information derived from several oculomotor types for better accuracy of output classes, and the custom eye-tracker nodes gather 3D oculomotor responses from a variety of stereo video stimulation sessions. The suggested technique showed an accuracy of 86 % for identifying Alzheimer's patients. To assess the learned models and enhance self-optimization of the training methods, intelligent model evaluation techniques could be included in future.

In order to help patients in regaining their confidence, Gao et al. [89] suggested an approach to identify anomalous behaviors associated with moderate cognitive impairment and forecast patient actions. In this approach, the home environment's architecture is formalized as an abstract grid. A user activity model (UAM) was built using a discrete-time Markov chain (DTMC) based on sensor data, in which everyday behaviors are verified using probabilistic computational tree logic (PCTL). A probabilistic model verification tool uses the UAM as input to compute probability values and evaluate temporal behavior. By identifying activities with unusual temporal characteristics or unexpected probability, the approach may also be used to diagnose problems. However, the user behavior model in this research was solely generated using DTMC and is unable to consider variations in these tasks over time and interruptions of some activities brought on by the forgetfulness of patients.

Three sensors and a Raspberry Pi were used in a smart cabinet to track the frequency of doors opened, providing a measure of the user's memory [90]. After putting the smart cupboard to the test in a controlled environment with 23 participants, a significant correlation was found between the results of the test and memory testing procedures. Validated face-name association memory test findings and a self-reported test of perceived memory were used to evaluate the accuracy of the memory tests. The proposed smart cabinet performed well in the memory test. The fact that the user is assumed to be the system's sole consumer is a weakness of the existing approach. Therefore, a system of identification that can locate a person is necessary.

5.6. Heart disease

Several heart monitoring apps have been used to test the IoMT system's data fusion capabilities. An electrocardiogram (ECG) can aid in the diagnosis of heart diseases, such as arrhythmias and coronary artery disease. For remote ECG monitoring, an IoT-authorized, cloud-oriented system was proposed by Raheja and Manocha [91]. To remove noise and identify ECG characteristic spots, the ECG signals are pre-processed using Savitzky-Golay and maximum overlap discrete wavelet packet transform. A triple data encryption standard is employed for encryption and authentication, and the CNN algorithm was developed for classification tasks. Cardiologists were given access to encrypted and authorized ECG data through the ThingSpeak platform for analysis. The proposed CNN model showed an average accuracy of 99.12 % when classifying heartbeats into five distinct forms of arrhythmias.

The IoMT in heart disease screening systems enables individuals to conduct self-examinations to evaluate the presence of irregularities in their hearts, thereby facilitating early detection of heart disease. As demonstrated by Su et al. [92], the screening system for valvular heart disease effectively examines and evaluates the distinctive signal values of individuals diagnosed with this condition. To enhance the prediction of patients' heart disease, Pan et al. [93] suggested an Enhanced Deep Learning assisted CNN (EDCNN) model. The EDCNN's hyperparameters were tuned after being designed to be as adaptable as possible, allowing for an accuracy of up to 99.1 %.

To develop a deep learning-based method for predicting heart diseases, Rajkumar et al. [94] focused on a publically available dataset on heart ailment in Hungary collected from Internet of Things (IoT) sensor devices. Using a modified deep long short-term memory (MDLSTM) method, the data are preprocessed, feature-selected, and categorized. The output is then modified by an improved spotted-hyena optimization technique. Python, where this method was implemented, has been shown to be accurate to within 0.01 % across a range of metrics. Further investigation into prenatal health and family history may aid in the detection of heart disease.

Lalitha & Jinny [95] proposed a hybrid architectural framework and ML model for predicting heart disease in medical settings based on

IoMT. Medical records were collected by utilizing IoMT devices in the proposed architecture. Categorical information was encoded with a one-hot mechanism and normalized with the help of a tried-and-true scalar technique during the preprocessing stage. Additionally, a hybrid sequence of Filter, Ensemble, and Wrapper approach was used to select the most important features. Logistic Regression and the Extreme Gradient Boosting (XGBoosting) algorithm both produced highly precise predictions, with an accuracy of 86.47 % and 85.81 %, respectively. The proposed model demonstrated a higher level of accuracy (80.53 %) when utilizing the decision tree approach in comparison to the existing approach (73.22 %).

A recent study by Basak and Chatterjee [96] discusses the development of a smart healthcare surveillance (SHS) system for heart diseases that integrates IoT and ML technologies to monitor and analyze vital signs data. Using ML techniques like Random Forest, Gaussian NB, Logistic Regression, Decision Tree, KNN, and SVM, the study predicted heart disease across all three layers of the proposed architecture, with Random Forest obtaining the greatest accuracy of 92.4 %. Deep learning models could be implemented to ensure the reliability of the method.

Integrating IoT, fog, and cloud, the FRIEND system was introduced by Pati et al. [97] to provide real-time remote diagnostics for heart patients. The system incorporated fog computing concepts and was found to be both user- and energy-friendly. The system was further evaluated using several machine learning algorithms and ensemble approaches and trained on a composite dataset comprised of several heart disease datasets, yielding a high accuracy of 94.27 % and other positive performance metrics. Despite its usefulness, the study has some drawbacks, such as a high price tag, limited data, and reliance on just one platform. The surveyed studies that were conducted on applications of data fusion in IoMT are summarized in Table 4.

In general, IoMT applications for data fusion make it possible for healthcare providers to employ large amounts of health data provided by linked devices and systems. Integrating and analyzing this data allows medical personnel to generate insights that can be put into action, which in turn improves patient monitoring, enables predictive analytics, and improves decision-making, all of which contribute to better patient outcomes.

6. Security issues in IoMT and potential solution

The healthcare sector has been transformed by IoMT through the interconnection of medical devices and systems to improve patient care and outcomes. However, this connectivity also raises security issues that must be addressed in order to protect individual patients' information, medical equipment, and the security of healthcare networks as a whole. One of the primary hurdles is the vulnerability of IoMT devices to cyber attacks, including unauthorized access, data breaches, and malicious tampering. Security of protocols, bioinformatics, and health data has become of the utmost importance due to the potential severity of an attack on the healthcare system, particularly the loss of control over life-supporting equipment [98]. The key security issues in IoMT include authentication, authorization, data confidentiality, availability, and integrity, as illustrated in Fig. 4.

Various approaches have been investigated to protect the healthcare system from being exploited through vulnerabilities, such as utilizing a blockchain-based environment for the IoMT and edge cloud technology [19,99]. Other potential solutions involve intense encryption implementation and authentication methods, regular software updates and patches, thorough risk assessments, training healthcare professionals on cybersecurity best practices, and establishing comprehensive regulatory frameworks to ensure adherence and responsibility [100–102]. Furthermore, fostering collaboration among manufacturers, healthcare providers, and cybersecurity experts is essential for resilient and secure IoMT system development that prioritizes the privacy of patients.

Table 4
Surveyed studies on the applications of data fusion in IoMT.

Application	Objective	Outcome	Remarks	Ref.
Remote Surgery	To investigate the use of enhanced 5 G robot-supported laparoscopic surgery in urology.	Enhanced robot-assisted laparoscopic telesurgery using 5 G technologies was found to be a practical, secure, and successful method for urological treatments.	The retrospective nature of the study and the relatively small sample size are two issues that need to be addressed.	[77]
	To propose an intensive care unit (ICU) teleultrasound diagnostic system.	Kidneys, gallbladders, spleens, livers, and pancreas were imaged using ultrasound technology performed on 32 patients. Success with the experiment was achieved.	The image quality was quite high-quality.	[78]
Epilepsy seizure detection	Automated identification of epileptic seizures in the IoMT using EEG data.	The efficacy of the suggested framework for detection, efficiency of resources, and scalability was demonstrated, justifying its implementation in the IoMT.	Decisions made during the identification of epileptic episodes are not easily understood. Possible benefits of explainable AI include the ability to generate visual or verbal explanations for detection decisions.	[79]
	To identify epileptic seizures while EEG data is compressed without any loss.	The compression power was four times that of previous methods, and the accuracy was between 99.53 % and 99.99 %.	When comparing the KCHE to a non-compressed EEG data method, the latency rate is reduced by 84.6–88.2 % for different types of EEG data recordings.	[80]
	To propose a prototype monitoring system for Grand Mal Epilepsy Tonic-Clonic (GTC) seizures.	The system had an average accuracy of 83.0 % for detecting muscle spasms, 98.1 % for monitoring core body temperature, 95.4 % for monitoring heart rate, and 87.2 % for detecting falls.	Clustering analysis might be utilized to better categorize and tailor a patient's symptoms.	[81]
Digital Biomarker	Analyze how non-invasive wearable devices may be used to measure blood glucose levels (BGL) in diabetics.	High accuracy was achieved when estimating the correlation between glycemic measures and characteristics.	Considering a small number of individuals may not be reflective of the system's actual performance as a whole.	[82]
	To identify human	MEmoR achieved accuracies of	A lack of information on	[83]

(continued on next page)

Table 4 (*continued*)

Application	Objective	Outcome	Remarks	Ref.
	emotions in real-time by utilizing data from the Emotional IoT and a deep learning model called MEmoR.	83.79 and 81.54 % in the prediction of valence-arousal and discrete emotion, respectively.	individual behavior in changing environments prevents the development of real-time emotion detection models.	
	To diagnose depression using LSTM and SVM algorithms.	Depression was assessed by overlapping sliding windows on recordings of motor activity and a mix of statistics and deep learning-derived variables.	The field of behavioral health can benefit from further study that incorporates transfer learning models and other aspects.	[84]
Teledentistry	To prevent and identify dental caries in its early stages.	Cariogenic parameters, such as biofilm pH, biofilm presence, and oral cavity temperature, can be easily monitored with intraoral sensors that can be fitted to a variety of dental products.	The method is easy to apply at a community level.	[86]
	To compare remote clinical consultations (RCC) versus in-person consultations to determine which was more effective for restorative dentistry.	RCC was as efficient and secure as an in-person consultation, regardless of gender or age.	The intervention's cost-effectiveness, efficacy under all clinical circumstances, and GDPs' acceptability in a real primary care practice should be evaluated.	[87]
Alzheimer's detection	To detect Alzheimer's by employing eye-tracker and cloud-based diagnostics made possible by ML.	The proposed model demonstrated an accuracy of 86 % for identifying Alzheimer's patients.	To assess the learned models and enhance self-optimization of the training methods, intelligent model evaluation techniques could be included in future.	[88]
	To identify anomalous behaviors associated with moderate cognitive impairment and forecast patient actions.	By identifying activities with unusual temporal characteristics or unexpected probability, the approach may be used to diagnose problems associated with Alzheimer's disease.	This model is unable to account for variations in several behavior tasks over time and interruptions in some activities caused by the forgetfulness of patients.	[89]
	To measure a user's memory.	The proposed smart cabinet performed well in a memory test.	The current implementation of the system implies there is only one user, which is one of the limitations.	[90]
Heart disease	To propose an IoT-authorized, cloud-oriented system for monitoring ECG remotely.	The proposed CNN model had an average accuracy of 99.12 % when classifying heartbeats into five distinct forms of arrhythmias.	More categories of arrhythmias could be analyzed in the future.	[91]
	To provide a heart disease prediction system based on deep learning.	The proposed model showed 98.01 % accuracy in predicting heart disease.	The research can be expanded to examine early hereditary and health-related characteristics for the early diagnosis of heart disease.	[94]
	To evaluate vital signs data in order to develop an SHS system for heart disease.	The model used ML algorithms and achieved 92.4 % accuracy.	Deep learning models could be implemented to verify the reliability of the method.	[96]
	To provide real-time remote diagnostics of heart patients.	The system was found to be both user- and energy-friendly by incorporating fog computing concepts.	Several issues need addressing, including high prices, limited data collection, and reliance on a single platform.	[97]

6.1. Security issues in IoMT

IoMT is susceptible to numerous vulnerabilities due to resource limitations in the devices, their diversity, and the sheer number of IoMT users. IoMT security needs fall into three main categories: function security, access control security, and information security. These security requirements are interconnected and reciprocally influenced by one another [103].

6.1.1. Authentication

Authentication challenges in IoMT refer to the difficulties in verifying the identity of devices, users, and data within the healthcare ecosystem. Given the complexity and diverse perspectives of IoMT systems, proposing universal authentication solutions for different nodes within these systems is challenging. Consequently, IoMT authentication primarily focuses on three levels, namely the device, network, and user levels [104]. Users at the application layer, such as patients and healthcare providers, are the primary emphasis of user-level authentication, whereas devices within the IoMT system are the main focus of device-level authentication [105–108]. Besides, network-level authentication involves registering and authenticating users and devices to ensure the inclusive security of the IoMT [109,110].

The main reason for using authentication techniques is to restrict IoMT's resources, features, facilities, and services to only those who are authorized to use them. As a result, it is crucial to evaluate authentication solutions' robustness in the face of potential attacks aimed at gaining unauthorized access to IoMT systems. Common IoMT authentication attacks include forgery attacks, smart card theft, insider attacks, tracking attacks, sensor attacks, Denial-of-Service (DoS) attacks, session key information breaches, Man-in-the-Middle (MitM) attacks, and dy-synchronization, among others [104]. ECG-based authentication has gained substantial attention in smart healthcare systems due to its unique attributes, such as being inimitable, suitable, accessible, and comfortable for users. However, enhancing authentication accuracy, particularly in scenarios with massive users, poses a considerable

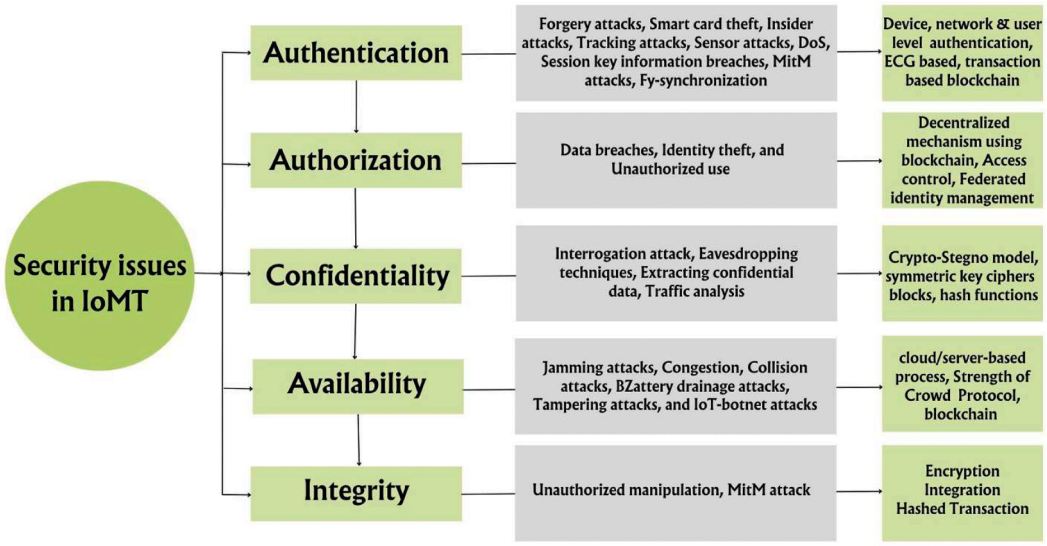

Fig. 4. Key security issues in IoMT.

challenge. A parallel ECG-based authentication method called PEA was introduced by Zhang et al. [111] to address this issue.

In addition to PEA, many models and strategies have been presented to deal with authentication attacks in this domain. For instance, Fotouhi et al. [112] devised a method that combines short-term and long-term parameters to safely generate and transfer a communication session key. These advancements aim to upgrade the security and effectiveness of ECG-based authentication systems for smart healthcare applications. Additionally, Hajian et al. [113] proposed an authentication strategy that effectively defends against guessing and insider attacks. In this scheme, the adversary is required to correctly guess three double-hashed values to pass the authentication process, making guessing attacks virtually impossible. Furthermore, Das [114] offered a method for resilience against MitM attacks that employs a temporal credential for secure communication between entities, preventing an adversary from exploiting the communication even if they possess other private credentials. In addition, the verifier in the proposed architecture is not predicated on the credentials provided during authentication.

Kumar and Tripathi [115] developed and improved a system that affects a transaction-based blockchain. By including time and identifier stamps on verified transactions, this scheme significantly reduces the likelihood of successful replay attempts. Sureshkumar et al. [116] introduced a method that effectively thwarts DoS attacks, making them difficult to execute. The scheme is based on request-response communication, in which the user must first receive a time-stamped approval from the sensor before a connection can be established. Bhuarya et al. [117], Das et al. [118], Tahir et al. [119], and Wu et al. [120] explored additional strategies and techniques to tackle the authentication and security issues in smart healthcare systems.

6.1.2. *Authorization*

During attacks, there is a risk of unauthorized access or data alteration to sensitive data that can result in the loss or unavailability of data for authorized users and customers. Authorization plays a central role in ensuring that solely authorized entities can access particular network resources, such as medical IoT devices and patient medical information. For example, committed entities are entitled to execute actions similar to giving commands to IoMT or upgrading device software [121]. Adversaries may exploit weak authorization techniques in an IoMT network to gain resources without proper rights. As a result of users' insufficient security training, knowledge, and awareness, social engineering attacks can exploit vulnerabilities in IoMT devices, allowing malicious actors to impersonate legitimate users and gain access to their medical devices. Attackers can use compromised IoMT devices as bots to initiate more attacks over the IoMT edge network and gain access to network services, such as remote control of numerous IoMT devices and important resources like patient medical data [122].

The consequences of inadequate authorization practices in IoMT can have critical implications, including data breaches, identity theft, and unauthorized use of sensitive medical information. Implementing robust authorization practices is essential to protect patient data and maintain the trust of individuals and organizations relying on IoMT systems. In the case of medical devices that monitor vital signs, compromised authorization can even harm a patient's life. Access control is a widely used security strategy that confirms proper authorization. An instance of an access control mechanism is an access control list (ACL), which is based on the concept of discretionary access control models using an access matrix. ACLs determine the specific operations that a verified user is authorized to access, retrieve, and execute [123]. These mechanisms provide granular control over access rights, enabling administrators to define and enforce permissions based on individual users or groups.

The centralized authorization server in traditional access control systems can pose challenges as being a single point of failure or a performance bottleneck. Hence, Xu et al. [124] developed a decentralized mechanism called BlendCAC using blockchain technology, which utilizes token management for various actions, enabling decentralized authorization decisions. This approach aligns with access control models commonly used in distributed architectures, where the access control logic is distributed and embedded within end devices rather than relying on a central authority [125]. The proposed BlendCAC scheme introduces a robust identity-based capability token management strategy that leverages smart contracts for propagation, revocation, and registration of access authorization. Instead of depending on oversight from a central authority, BlendCAC allows IoMT devices to manage their resources autonomously. To assess the effectiveness of the strategy, BlendCAC was deployed to Raspberry Pi and evaluated on a private blockchain network in the area. The results showcase the viability and potential of BlendCAC to provide a scalable, lightweight, decentralized, and fine-grained access control solution for IoMT [124]. By leveraging blockchain technology and decentralizing the authorization process, BlendCAC offers the potential to enhance scalability, resilience, and performance in access control systems.

Federated identity management facilitates the secure federation of identities across various healthcare organizations, thereby reducing the need for individual management of user identities. This can alleviate

administrative burdens and ensure the security of identity-related processes within IoMT. Moreover, adopting safe protocols, such as Transport Layer Security (TLS), guarantees the establishment of secure communication channels between IoMT devices and systems. TLS safeguards data integrity and confidentiality, effectively preventing any unauthorized interception of data during transmission. By incorporating federated identity management and robust protocols like TLS, the IoMT environment can benefit from enhanced identity security and protected communication for data exchange [126].

6.1.3. Data confidentiality

Ensuring the confidentiality of data within IoMT is of utmost importance due to the sensitive features of medical data. IoMT encompasses an interconnected network of medical systems, devices, and sensors that collect and transmit health-related information. Confidentiality entails the safety of a patient's medical data shared with therapists, physicians, and medical personnel from unauthorized disclosure to individuals who may misuse or harm the patient or exploit the data inappropriately [21]. To illustrate, if the confidentiality of transferred information is compromised, an antagonist could intervene between the sender and receiver, intercept the medical data being transmitted, and gain access to restricted information. Preserving the integrity of healthcare technologies and devices against potential attacks is crucial, and there is a pressing need for improvements in traditional systems to mitigate these risks. Consequently, extensive efforts are dedicated to developing multiple solutions in this domain. Regarding data confidentiality, blockchains facilitate interested parties within a given network to access information while enforcing stringent security measures, such as role-based and attribute-based policies. Regrettably, there have been numerous instances where patient data has been left vulnerable [127].

The IoMT edge network encompasses IoT devices with limited resources that strike challenges for implementing resource-intensive cryptographic solutions like data encryption/decryption. Therefore, it becomes challenging to maintain a high data secrecy level, making the network vulnerable to threats that aim to compromise the privacy of transferred or stored information [121]. For instance, an attacker can use eavesdropping techniques to monitor communications and examine the contents of transferred data packages within the IoMT edge network. The adversary can then passively capture the conversation between the wearable sensor and IoMT gateway and, by traffic analysis or other means, extract private information [128].

Interrogation attacks involving impersonation pose a significant risk to data confidentiality [122]. In this scenario, a malicious actor masquerades as a legitimate system, redirecting requests to other entities solely to expose private information about users. Numerous methods are available to verify data confidentiality, spanning from physical safeguards to cryptographic algorithms that obfuscate information. Cryptography pertains to concealing communication practices to enhance the confidentiality of stored data, offering various encoding schemes that add protection when transmitting information through open channels or interconnected systems. However, relying solely on cryptography is insufficient to guarantee comprehensive information security. Thus, alternative approaches, such as steganography, are necessary to mitigate risks. Steganography, closely related to cryptography, provides an additional layer of protection. Different types of steganography algorithms can be identified by the methods they use to embed and retrieve information [129,130]. A novel Crypto-Stegno model was introduced by Li et al. [130] to safeguard medical information within the IoMT environment. The study validated the effectiveness of using healthcare information datasets and demonstrated exceptional outcomes in terms of perceptibility quality, resilience against data loss, embedding capacity, and overall security. These remarkable results establish the Crypto-Stegno system as a reliable and efficient approach for securing medical information within the IoMT platform.

Secure communication between low-power IoMT devices like medical sensors and nodes is possible with the help of a variety of lightweight cryptographic algorithms. These include symmetric key ciphers like block and stream ciphers, as well as hash functions [131]. However, key ciphers face challenges related to the distribution of keys, which is a crucial aspect of cryptographic security. The evolving nature of cyber threats demands ongoing monitoring, auditing, and incident response plans to detect and address potential breaches promptly. Achieving and maintaining data confidentiality in IoMT is an ongoing challenge that necessitates a holistic and proactive approach to protect sensitive medical information and safeguard patient trust.

6.1.4. Availability

The interruption of correct operations and impeded access to medical information significantly impact the availability of data, potentially resulting in life-threatening consequences. This feature indicates the accessibility of IoMT services, whereby authorized users may encounter unavailability of data when requesting access to these services. Particularly in healthcare systems where constant monitoring of a patient's health is paramount, the availability aspect assumes crucial importance [128]. Specifically, availability assures that the information is exclusively accessible to authorized entities. Nevertheless, healthcare systems that heavily rely on IoMT devices face resource and computational constraints, thereby posing challenges to the preservation of service availability.

In cases where an attacker cannot compromise the confidentiality and integrity of ongoing communication within the IoMT system, they may resort to launching alternative attacks. These include jamming attacks, congestion, collision attacks, battery drainage attacks, tampering attacks, and IoT-botnet attacks, which can be directed at various network layers impacting the IoMT edge network. A battery drainage attack can be executed by a malicious person who intentionally sends deceptive content to the targeted device, causing excessive power consumption and depletion of the device's battery [132]. Collision attacks occur when two nodes concurrently transfer data on a shared frequency channel, leading to an identification conflict at the receiving end. Consequently, corrupted received data packets are discarded, resulting in the retransfer of the packets and the waste of network resources within the IoMT [133].

Numerous research efforts have concentrated on centralized or partially centralized approaches and solutions aimed at mitigating jamming attacks [134,135]. Xuan et al. [136] introduced a trigger identification service to defend against susceptible jammers, which identifies and distinguishes nodes that exhibit transmission behavior similar to the jamming nodes. The authors utilized optimization problems to create a comprehensive framework for trigger identification in unreliable wireless sensor networks. They also proposed an improved algorithm to enhance the scheme's robustness in various network scenarios, particularly when facing sophisticated jamming models. While this scheme effectively counters malicious actions, it relies on cloud or server-based decision-making processes.

Although pattern recognition algorithms applied to node transmissions demonstrate promising potential, using a centralized system is essential to manage computational costs. Additionally, the Strength of Crowd (SoC) procedure offers a distributed solution, which is particularly suitable for IoMT devices with limited resources. It also assures message distribution to the intended receiving nodes, despite the blocking of a substantial portion of the available bandwidth. Specifically, the SoC protocol relies on a strategy of deception, where legitimate devices transmit deceptive packets into the network, confusing potential jammers and making it challenging to differentiate between genuine and false nodes [137]. Another approach by Liu and Sun [138] involves a lightweight algorithm, which is capable of recognizing patterns or behaviors, coupled with a notification system. This combination enables the detection of unusual activities within the IoMT environment.

To guarantee the accessibility of various IoMT applications, several case studies have implemented blockchain technology, which expedites

access to sources and services via forecasting and management [139]. Using hash functions for profile matching, Nie et al. [140] investigated the authentication of private data in IoMT while addressing the issue of physical layer availability. In order to facilitate safe data sharing, the authors implemented encryption methods and outlined a secret key for profile matching. The study also introduced an optimized pricing mechanism to incentivize greater user participation in health data sharing and maximize user profitability. Furthermore, an inspection demonstrated that the proposed approach effectively meets various security objectives within IoMT scenarios.

6.1.5. Integrity

Integrity ensures the authenticity and accuracy of data, guaranteeing that received messages are free from false information, unauthorized modifications, and deletions during communication. Within the context of IoMT, integrity concerns revolve around the accuracy, dependability, and coherence of produced, transmitted, and processed data and information by interconnected medical devices and systems. The productive integration of IoMT networks within the medical field also heavily relies on upholding the integrity of the associated devices (e.g., wearable or implantable sensors inside the human body). Nonetheless, because IoMT devices commonly function within environments lacking trust, they are susceptible to physical assaults aiming to compromise device integrity [122]. These concerns may have serious effects on patient security and the quality of services provided. Unauthorized tampering or manipulation of medical data can result in erroneous diagnoses, inappropriate treatments, and inadequate patient care. For instance, altering vital signs or laboratory test results can mislead healthcare professionals, leading to inaccurate medical decisions and potentially detrimental outcomes.

A man-in-the-middle (MitM) attack is an assault that threatens the integrity of IoMT networks. An intruder in this scenario could secretly listen in on a conversation between two parties, manipulating information without raising suspicion [121]. For instance, in IoMT edge networks, the gathered medical data can be either stored locally or transferred to a remote server within the devices' internal memory. During transmission, data becomes vulnerable to interception and modification by a MitM attacker, which ultimately compromises the integrity of the data [141,142].

Seliem and Elgazzar [143] proposed a method for protecting confidentiality that makes use of a network cluster, cloud server, smart medical appliances, and medical facilities. All transactions within the system are hashed, and only the data holders possess the corresponding hash values to ensure integrity. This method provides robust security measures, even in situations where communication channels are compromised. However, using cryptography and transaction handling in this approach causes increased power consumption due to additional computational overhead. Another way to securely store health data is by leveraging the characteristics of blockchain technology. Blockchain offers features like distributed architecture (eliminating a single point of failure), transparency, near-immutability, secure cryptography, and the ability to utilize smart contracts. These characteristics make blockchain the preferred mechanism for ensuring data integrity in the IoMT Cloud [144].

The secure framework for IoMT presented by Rathnayake et al. [145] focuses on the key privacy, security, and sensor data integrity issues. The framework, operating within a cloud-mobile architecture, relies on three encryption processes: Proven Data Possession (PDP), Attribute-Based, and Advanced Data Encryption. Utilizing these encryption methods and leveraging cloud technologies, the proposed model successfully addresses the specific challenges associated with medical applications. Notably, the PDP technique confirms the integrity of encrypted files using AES and ABE. This approach facilitates users to verify the presence of their information on the server without the retrieval of the entire dataset. Additionally, key exchange is facilitated through in-band protocols in the suggested framework.

To protect data during transit over the IoMT's edge network, Lounis et al. [146] proposed a hybrid strategy utilizing symmetric cryptography and attribute-based encryption (ABE). The shared messages undergo initial encryption using a randomly generated symmetric key (RSK) and are encrypted further using ABE. If an IoMT device possesses the appropriate secret key that fulfills the access policy of ABE, the message and RSK can be decrypted. The private key is associated with the attribute set of the device, representing the user's advantages. Notably, by legitimately modifying the system's configuration, there is an opportunity to encrypt only the downloaded RSK rather than the whole message, resulting in improved communication efficiency and reduced costs [147].

There are many ways in which healthcare can benefit from IoMT, but the field also faces new challenges. For instance, authentication and authorization issues emerge in the context of IoMT devices and systems, necessitating rigorous verification and control mechanisms for accessing sensitive patient data and devices. Maintaining patients' confidence and complying with strict privacy regulations are at the forefront of privacy concerns related to protecting large amounts of private medical information from unauthorized access and breaches. Since interruptions or outages in the connectivity of medical devices can have potentially serious consequences, availability issues necessitate that IoMT systems remain consistently operational and accessible. Finally, data integrity must be maintained to ensure that health data is accurate and unchanged throughout the transmission and storage processes, which is crucial for facilitating well-informed medical decision-making and protecting patient safety. The effective and secure integration of IoMT into healthcare ecosystems necessitates addressing these complex challenges.

As the medical sector embraces IoT solutions, it is evident that some manufacturers are rushing to adopt these technologies without prioritizing security measures. This lack of emphasis on security induces security concerns regarding data/software. Future studies should prioritize addressing security, privacy, risk assessment, standardization, interoperability, and ethical considerations in IoMT deployments. These aspects are crucial for ensuring the authentication, authorization, confidentiality, integrity, and availability of medical data and systems while promoting responsible and effective use of IoT technologies.

6.2. Potential solutions to the security issues in IoMT

Healthcare institutions must guarantee that their devices are secure from current threats, given the various ways that hackers might compromise security and negatively impact clinical operations by gaining access to clinical equipment [148]. There are a number of potential solutions that could be used to address the security issues in IoMT, including securing communication protocols like TLS or datagram TLS to secure and authenticate data transferred between IoMT devices and systems. Strong authentication methods, such as multi-factor authentication, can also improve security by confirming the identity of users and devices [149]. Utilizing powerful encryption methods helps to protect sensitive data both in transit and at rest.

A complete solution for collecting, protecting, and storing data in the IoMT should include both technical solutions and best practices. To provide patients with healthcare services, it is necessary to collect, retain, and analyze private medical data to correspond with the General Data Protection Regulation (GDPR). Key security solutions for collecting, protecting and storing data in the IoMT are outlined below:

(i) Data backup and recovery: This is the process of saving copies of data so that it can be restored in the event of data loss or a system crash. Data loss can be prevented with the use of off-site storage and redundant backup systems. Test the data restoration procedure to ensure it can be relied upon.
(ii) Secure protocols: Use encrypted connections between devices and gateways by employing secure communication protocols like

TLS or datagram TLS. These protocols allow for authenticated and verified delivery of data without compromising its security or integrity.

(iii) Encryption: Use robust cryptographic techniques to encrypt data from beginning to end. As part of this process, data are encrypted at the sending device, sent securely through networks, and then decrypted at the receiving device. Both the medium of transmission and the content of the data being transmitted should be encrypted.

(iv) Access control: Use robust mechanisms for access control to manage data transfer within the IoMT ecosystem. Role-based access control (RBAC) can be used to restrict data transmission and reception to approved people and devices. Data transmission can be isolated and protected by using network segmentation and virtual private networks (VPNs).

(v) Mutual authentication: To ensure the integrity of all communications, it is important to implement mutual authentication across all devices and gateways. This reduces the likelihood of attacks from malicious software or hardware by making it possible for all parties involved in a transaction to verify each other's identities before any data is exchanged.

(vi) Intrusion prevention and detection: Organize intrusion prevention and detection systems to keep tabs on network activity and spot signs of hacking. Unauthorised login attempts and unusual data patterns are two examples of what these systems can detect to send out alerts about or even take preventative measures against.

(vii) Data loss prevention: Put preventative measures in place. To prevent the loss of vital medical records, it is necessary to take measures like keeping backups, establishing systems to handle packet loss, and assuring data retransmission or redundancy.

(viii) Data lifecycle management: Define the collection, storage, access, and deletion of data inside the IoMT infrastructure and provide unambiguous data lifecycle management policies. To protect user privacy and remain in regulatory compliance, it is important to implement data retention policies, data archiving protocols, and secure data disposal techniques.

(ix) Traffic monitoring and analysis: Use network monitoring tools to keep tabs on data flows and look for anything out of the ordinary that could pose a security risk. This allows for continuous tracking of data transfers and the early detection of any suspicious activities.

(x) Security audits and testing: Perform routine security audits and penetration testing to locate security holes in the IoMT platform. Assessing the security posture of a system beforehand allows businesses to pinpoint vulnerabilities and implement fixes that better protect sensitive information during transit.

(xi) Checks for data integrity: Implement procedures to ensure that data is accurate. Checksums, digital signatures, and hash functions are examples of techniques that can be used to protect data from being altered without detection. In order to detect data integrity breaches, regular integrity tests should be performed.

(xii) Security awareness and training: Inform medical staff, IT managers, and end users of recommended practices for keeping sensitive information safe throughout transmission. Regular training sessions should be held to ensure that all employees know how to handle sensitive information safely and securely while in transit. Use encrypted connections between devices and gateways by employing secure communication protocols like TLS or datagram TLS. These protocols allow for authenticated and verified delivery of data without compromising its security or integrity.

(xiii) Firmware and software updates: Update the firmware and software on your IoMT devices, gateways, and network infrastructure on a regular basis. This protects the system from any new threats that may arise by applying the latest security updates and fixing any known vulnerabilities.

By adopting these data transportation security solutions, healthcare providers may better protect patient data, uphold the IoMT ecosystem, and reduce the likelihood of data breaches caused by hacking, eavesdropping, or other forms of malicious activity. In conclusion, addressing security concerns with IoMT calls for a multi-pronged strategy that incorporates robust authentication systems, encryption, privacy-enhancing technology, standardized security procedures, patch management strategies, and employee education and training. It is essential for manufacturers, healthcare organizations, regulatory agencies, and cybersecurity specialists to work together to secure patient data and ensure the security and privacy of IoMT systems.

7. Open issues and challenges in IoMT

Connecting medical devices, sensors, and healthcare systems through the IoMT has the potential to revolutionize healthcare by enhancing patient care and streamlining administrative tasks. However, for the IoMT ecosystem to be widely adopted and successful, several open issues and challenges must be resolved. Some of the most significant obstacles include:

- Protecting the privacy and confidentiality of patient information is of utmost importance in the healthcare industry. The risk of data breaches and unauthorised access is becoming increasingly important as the number of connected devices and data transmission increases.
- The consequences of a healthcare system going down or a medical device breaking can be devastating. It is crucial to guarantee the dependability and accessibility of IoMT tools and infrastructure.
- The quality and accuracy of the data collected by IoMT devices are essential in enabling knowledgeable medical decision-making. Maintaining trustworthy and accurate data is an ongoing issue.
- The devices and systems that comprise IoMT frequently come from various vendors and employ different communication protocols, raising the issue of interoperability. However, ensuring that all of these devices can communicate with one another and exchange data without any difficulties is no easy task.
- As the number of connected devices and data sets increases, it can be difficult to effectively manage and scale the underlying infrastructure supporting the IoMT ecosystem.
- The proper use of IoMT devices and the interpretation of the data they produce calls for proper training and education on the part of healthcare professionals. It can be challenging to make sure everyone working in healthcare has sufficient education.
- Patients must have faith in IoMT tools and infrastructure for it to be useful. Trust from patients must be earned and kept over time.
- Delays in rolling out IoMT solutions can be caused by a lack of suitable infrastructure and unreliable connectivity in some areas, especially rural ones.
- Although there have been some successful attempts to standardize IoMT technologies, there is still a lack of universal standards that can make it difficult for different IoMT technologies to work together smoothly.
- Life-threatening consequences could result from hacking or unauthorised access to medical devices, making it imperative to ensure their security.
- Some ethical issues arise when using IoMT, including patient consent, data misuse, and the ethical relevance of AI-driven diagnoses and treatment suggestions.
- The issue of ascertaining ownership and control of data generated by IoMT devices presents an ongoing challenge, with the question of whether it belongs to the healthcare provider, patient, or device manufacturer yet to be definitively resolved.

To overcome the issues mentioned above, the device manufacturers, healthcare community, technologists, and regulators must work

together. New difficulties and prospects are likely to arise as the field of IoMT develops further, highlighting the importance of continuing research and development.

8. Future directions in IoMT research

With the advancement of new network security technologies and the creation of additional digital medical devices, IoMT is constantly evolving. Future studies should concentrate on the issues mentioned below.

- IoMT has no set architecture that must be adhered to by everyone who develops IoT applications. Some gadgets, including CCTV cameras and field sensors, lack the ability to update their software, making them security-wise obsolete after a certain period of time. As a result, newer, more modern versions must be used in their place. Therefore, future studies should investigate the possibility of upgrading these devices when they are connected to the IoMT to reduce the implementation cost of visual surveillance over the IoMT.
- Protecting the IoMT application requires secure communication channels, early identification of system faults, and the installation of the right software and hardware. These regulations are essential to the organization's effective operation. Since IoMT involves a variety of more private and sensitive data, it is crucial to identify which patient data require the patient's specific consent for access in order to protect his or her fundamental rights. As a result, future adoption of effective policy tailored specifically for the IoMT is required.
- IoMT places a lot of importance on network research. Channel-based attacks can damage the integrity of the original data and, thus, are extremely dangerous because they could happen while the data is in transit. The variability of the IoMT environment makes it challenging to implement malware detection solutions. In a cross-platform environment, it is challenging to build tools and procedures that can detect malware. For instance, the system would become more complex and malware would be tougher to discover if data and information were transferred from smart homes to smart healthcare systems for patient monitoring. Consequently, continuous network-based malware strategies must be created.
- IoMT is comprised of a wide range of devices, applications, networks, and data transport paradigms, each with its own unique set of features and requirements. As a consequence, finding malware is a really difficult task. One method to address heterogeneity issues in the IoMT is to utilize an "electronic health recorder" to store user data over an IoT-based cloud for processing. In the IoMT setting, the BAN also generates a tremendous amount of information. Consequently, a more focused strategy needs to be developed in order to detect malware in a setting this complicated. Moreover, each device has a unique operating system, range of communication, storage capacity, and power consumption. Therefore, a more specialised approach to attack detection in such a system needs to be developed.
- IoMT-based systems contain a sizeable amount of confidential and sensitive data, which continues to grow with time. The security of a system based on IoMT might be strengthened in several ways, including through the use of cryptography and blockchain technology. Data integrity is improved by using SHA-256 efficiently. Blockchain technology is being employed in a variety of technological disciplines, and its application in the Internet of Things would be very helpful in ensuring data integrity. Moreover, the IoMT-based technology uses extremely sensitive data. Patients are the sole controllers of such data, excluding healthcare professionals. As a result, there is always a possibility of data leakage. The time-stamped feature of blockchain technology could prove invaluable for verifying the accuracy of such records. Once these records are stored on a decentralized ledger, it will be easier to identify anomalies in patient data.
- Detecting malware in cross-platform IoMT systems is a significant challenge that must be met to ensure the safety of patients, the confidentiality of personal information, and the reliability of healthcare services as a whole. There needs to be more study done in this area to prevent safety issues and other problems with IoMT in healthcare from impeding its usefulness.

System software and application software play a crucial role in facilitating a wide range of medical processes by acting as bridges between the software and hardware layers, respectively. Consequently, the research and development in this domain emerge as a critical area of focus for ensuring IoMT's smooth functioning. It is critical to regularly detect any defects in the codes of these programs; hence, a standardized proper framework is required to design the security monitoring system in the software. The operating system code in IoMT devices must also be analysed to detect the presence of zero-day threats.

9. Conclusion

The applications of IoT and IoMT continue to expand daily in a wide range of platforms for exchanging information in multiple industries. IoMT is increasing the amount of available data from numerous sources, including clinical systems, wearables, electronic health records, and medical devices. Data fusion involves integrating these diverse data sources, such as imaging scans and laboratory results, to generate a more comprehensive picture of a patient's health status. This allows healthcare providers to establish more precise diagnoses and treatment plans. The accuracy of predictions is directly impacted by the quality, quantity, and relevance of the data obtained from IoMT devices. While the multimodal emotion recognition (MEmoR) model provided a minimum accuracy of 81.54 % in predicting discrete emotion, the Epilepsy seizure detector-based Naive Bayes (ESDNB) algorithm was found to be the most effective for detecting epileptic seizures in IoMT networks, with an accuracy of 99.53 % to 99.99 %. However, IoMT faces a number of challenges with data fusion. Data standardization is essential due to the fact that data from numerous systems and devices may be stored in different formats, making it difficult to integrate and analyze. Privacy and security issues are major concerns since data sent via the Internet are vulnerable to hacking and unauthorised access. There is also an important need to revolutionize how data are collected, transported, and stored.

CRediT authorship contribution statement

Shams Forruque Ahmed: Conceptualization, Writing – original draft, Supervision. **Md. Sakib Bin Alam:** Methodology, Writing – original draft. **Shaila Afrin:** Writing – original draft, Validation. **Sabiha Jannat Rafa:** Writing – original draft, Data curation. **Nazifa Rafa:** Writing – original draft, Formal analysis. **Amir H. Gandomi:** Writing – review & editing, Supervision.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgments

The authors highly express their gratitude to the Asian University for Women, Chattogram, Bangladesh, for their support in carrying out this

study.

References

[1] A. Rahman, M.S. Hossain, G. Muhammad, D. Kundu, T. Debnath, M. Rahman, M. S.I. Khan, P. Tiwari, S.S. Band, Federated learning-based AI approaches in smart healthcare: concepts, taxonomies, challenges and open issues, Cluster Comput. 26 (2023) 2271–2311.

[2] S. Vishnu, S.R. Jino Ramson, R. Jegan, Internet of Medical Things (IoMT)-an overview, in: ICDCS 2020 - 2020 5th Int. Conf. Devices, Circuits Syst, 2020, pp. 101–104, https://doi.org/10.1109/ICDCS48716.2020.243558.

[3] M.M. Islam, S. Nooruddin, F. Karray, G. Muhammad, Internet of Things: device capabilities, architectures, protocols, and smart applications in healthcare domain, IEEE Internet Things J 10 (4) (2022) 3611–3641.

[4] A. Si-Ahmed, M.A. Al-Garadi, N. Boustia, Survey of machine learning based intrusion detection methods for Internet of Medical Things, Appl. Soft Comput. 140 (2022), 110227, https://doi.org/10.1016/j.asoc.2023.110227.

[5] G. Muhammad, F. Alshehri, F. Karray, A. El Saddik, M. Alsulaiman, T.H. Falk, A comprehensive survey on multimodal medical signals fusion for smart healthcare systems, Inf. Fusion. 76 (2021), https://doi.org/10.1016/j.inffus.2021.06.007.

[6] L. Wang, Y. Ali, S. Nazir, M. Niazi, ISA evaluation framework for security of internet of health things system using AHP-TOPSIS methods, IEEE Access 8 (2020) 152316–152332, https://doi.org/10.1109/ACCESS.2020.3017221.

[7] J.N.S. Rubí, P.R.de L. Gondim, Interoperable Internet of Medical Things platform for e-Health applications, Int. J. Distrib. Sens. Netw. 16 (2020), https://doi.org/10.1177/1550147719889591.

[8] X. Li, H. Dai, Q. Wang, M. Imran, D. Li, M. Ali, Securing Internet of Medical Things with friendly-jamming schemes, Comput. Commun. 160 (2020) 431–442, https://doi.org/10.1016/j.comcom.2020.06.026.

[9] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, R. Jain, Recent advances in the Internet-of-Medical-Things (IoMT) systems security, IEEE Internet Things J. 8 (2021), https://doi.org/10.1109/JIOT.2020.3045653.

[10] B. Shanmugam, Risk Assessment of Heterogeneous IoMT Devices : a Review, 2023.

[11] W. Ding, X. Jing, Z. Yan, L.T. Yang, A survey on data fusion in internet of things: towards secure and privacy-preserving fusion, Inf. Fusion. 51 (2019) 129–144, https://doi.org/10.1016/j.inffus.2018.12.001.

[12] H. Lin, S. Garg, J. Hu, X. Wang, M. Jalil Piran, M.S. Hossain, Privacy-enhanced data fusion for COVID-19 applications in intelligent Internet of Medical Things, IEEE Internet Things J 8 (2021) 15683–15693, https://doi.org/10.1109/JIOT.2020.3033129.

[13] M. Al-Hawawreh, M.S. Hossain, A privacy-aware framework for detecting cyber attacks on internet of medical things systems using data fusion and quantum deep learning, Inf. Fusion. (2023), 101889.

[14] Y. Sun, F.P.W. Lo, B. Lo, Security and privacy for the Internet of Medical Things enabled healthcare systems: a survey, IEEE Access 7 (2019), https://doi.org/10.1109/ACCESS.2019.2960617.

[15] M. Wazid, A.K. Das, J.J.P.C. Rodrigues, S. Shetty, Y. Park, IoMT malware detection approaches: analysis and research challenges, IEEE Access 7 (2019) 182459–182476, https://doi.org/10.1109/ACCESS.2019.2960412.

[16] T. Yaqoob, H. Abbas, M. Atiquzzaman, Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices-a review, IEEE Commun. Surv. Tutorials. 21 (2019) 3723–3768, https://doi.org/10.1109/COMST.2019.2914094.

[17] P. Pratim, D. Dash, N. Kumar, Sensors for internet of medical things : state-of-the-art , security and privacy issues , challenges and future directions, Comput. Commun. 160 (2020) 111–131, https://doi.org/10.1016/j.comcom.2020.05.029.

[18] A. Hafizah, M. Aman, W. Haslina, S. Sameen, Journal of network and computer applications IoMT amid COVID-19 pandemic : application , architecture , technology , and security, J. Netw. Comput. Appl. 174 (2021), 102886, https://doi.org/10.1016/j.jnca.2020.102886.

[19] R. Dwivedi, D. Mehrotra, S. Chandra, Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: a systematic review, J. Oral Biol. Craniofacial Res. 12 (2022), https://doi.org/10.1016/j.jobcr.2021.11.010.

[20] P. Wal, A. Wal, N. Verma, R. Karunakakaran, A. Kapoor, Internet of Medical Things – the future of healthcare, Open Public Health J. 15 (2022) 1–9, https://doi.org/10.2174/18749445-v15-e221215-2022-142.

[21] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop, J. Rodriguez, D. Lymberopoulos, A survey on security threats and countermeasures in Internet of Medical Things (IoMT), Trans. Emerg. Telecommun. Technol. 33 (2022), https://doi.org/10.1002/ett.4049.

[22] Z. Ashfaq, A. Rafay, R. Mumtaz, S. Mohammad, H. Zaidi, H. Saleem, S. Ali, R. Zaidi, S. Mumtaz, A. Haque, A review of enabling technologies for Internet of Medical Things (IoMT) ecosystem, Ain Sham. Eng. J. 13 (2022), 101660, https://doi.org/10.1016/j.asej.2021.101660.

[23] A. Hemmati, A.M. Rahmani, Internet of Medical Things in the COVID-19 era: a systematic literature review, Sustain 14 (2022), https://doi.org/10.3390/su141912637.

[24] M.J. Sudha, S. Viveka, A comprehensive review of architecture, classification , challenges, and future of the Internet of Medical Things (IoMTs), Med. J. Babylon. 19 (2022) 311–317, https://doi.org/10.4103/MJBL.MJBL.

[25] F. Kamalov, B. Pourghebleh, M. Gheisari, Y. Liu, S. Moussa, Internet of Medical Things privacy and security: challenges, solutions, and future trends from a new perspective, Sustain 15 (2023), https://doi.org/10.3390/su15043317.

[26] B. Bhushan, A. Kumar, A.K. Agarwal, A. Kumar, P. Bhattacharya, A. Kumar, Towards a secure and sustainable Internet of Medical Things (IoMT): requirements, design challenges, security techniques, and future trends, Sustain 15 (2023), https://doi.org/10.3390/su15076177.

[27] S.F. Ahmed, N. Rafa, T. Mehnaz, B. Ahmed, N. Islam, M. Mofijur, A.T. Hoang, G. M. Shafiullah, Integration of phase change materials in improving the performance of heating, cooling, and clean energy storage systems: an overview, J. Clean. Prod. 364 (2022), 132639, https://doi.org/10.1016/j.jclepro.2022.132639.

[28] J.E. Ferguson, A.D. Redish, Wireless communication with implanted medical devices using the conductive properties of the body, Expert Rev. Med. Dev. 8 (2011) 427–433, https://doi.org/10.1586/erd.11.16.

[29] A. Kos, V. Milutinović, A. Umek, Challenges in wireless communication for connected sensors and wearable devices used in sport biofeedback applications, Futur. Gener. Comput. Syst. 92 (2019) 582–592, https://doi.org/10.1016/j.future.2018.03.032.

[30] T. Belkhouja, S. Sorour, M.S. Hefeida, Role-based hierarchical medical data encryption for implantable medical devices, in: 2019 IEEE Glob. Commun. Conf. GLOBECOM 2019 - Proc, 2019, pp. 1–6, https://doi.org/10.1109/GLOBECOM38437.2019.9014192.

[31] E. Meng, R. Sheybani, Insight: implantable medical devices, Lab. Chip. 14 (2014) 3233–3240, https://doi.org/10.1039/c4lc00127c.

[32] K.G. Tarakji, A.M. Zaidi, S.L. Zweibel, N. Varma, S.F. Sears, J. Allred, P. R. Roberts, N.A. Shaik, J.R. Silverstein, A. Maher, S. Mittal, A. Patwala, J. Schoenhard, M. Emert, G. Molon, G. Augello, N. Patel, H. Seide, A. Porfilio, B. Maus, S.L. Di Jorio, K. Holloman, A.C. Natera, M.P. Turakhia, Performance of first pacemaker to use smart device app for remote monitoring, Hear. Rhythm O_2 2 (2021) 463–471, https://doi.org/10.1016/j.hroo.2021.07.008.

[33] B. Priya Prathaban, R. Balasubramanian, R. Kalpana, ForeSeiz: an IoMT based headband for real-time epileptic seizure forecasting, Expert Syst. Appl. 188 (2022), 116083, https://doi.org/10.1016/j.eswa.2021.116083.

[34] M.A. Sayeed, S.P. Mohanty, E. Kougianos, H. Zaveri, IDDS: an edge-device in IoMT for automatic seizure control using on-time drug delivery, in: Dig. Tech. Pap. - IEEE Int. Conf. Consum. Electron. 2020-January, 2020, https://doi.org/10.1109/ICCE46568.2020.9043143.

[35] B.A. Alzahrani, A. Irshad, A. Albeshri, K. Alsubhi, A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks, Wirel. Pers. Commun. 117 (2021) 47–69, https://doi.org/10.1007/s11277-020-07237-x.

[36] P. Sasidharan, T. Rajalakshmi, U. Snekhalatha, Wearable cardiorespiratory monitoring device for heart attack prediction, in: Proc. 2019 IEEE Int. Conf. Commun. Signal Process. ICCSP 2019, 2019, pp. 54–57, https://doi.org/10.1109/ICCSP.2019.8698059.

[37] R. Lazazzera, Y. Belhaj, G. Carrault, A newwearable device for blood pressure estimation using photoplethysmogram, Sensors (Switzerland) 19 (2019) 1–18, https://doi.org/10.3390/s19112557.

[38] Q. Lin, W. Xu, J. Liu, A. Khamis, W. Hu, M. Hassan, A. Seneviratne, H2B: heartbeat-based secret key generation using piezo vibration sensors, in: IPSN 2019 - Proc. 2019 Inf. Process. Sens. Networks, 2019, pp. 265–276, https://doi.org/10.1145/3302506.3310406.

[39] R. López-Blanco, M.A. Velasco, A. Méndez-Guerrero, J.P. Romero, M.D. del Castillo, J.I. Serrano, E. Rocon, J. Benito-León, Smartwatch for the analysis of rest tremor in patients with Parkinson's disease, J. Neurol. Sci. 401 (2019) 37–42, https://doi.org/10.1016/j.jns.2019.04.011.

[40] H. Ryu, H. moon Park, M.K. Kim, B. Kim, H.S. Myoung, T.Y. Kim, H.J. Yoon, S. S. Kwak, J. Kim, T.H. Hwang, E.K. Choi, S.W. Kim, Self-rechargeable cardiac pacemaker system with triboelectric nanogenerators, Nat. Commun. 12 (2021) 1–9, https://doi.org/10.1038/s41467-021-24417-w.

[41] S. Panja, A.K. Chattopadhyay, A. Nag, J.P. Singh, Fuzzy-logic-based IoMT framework for COVID19 patient monitoring, Comput. Ind. Eng. 176 (2023), https://doi.org/10.1016/j.cie.2022.108941.

[42] S. Razdan, S. Sharma, Internet of Medical Things (IoMT): overview, emerging technologies, and case studies, in: IETE Tech. Rev. (Institution Electron. Telecommun. Eng. India), 2022, p. 39, https://doi.org/10.1080/02564602.2021.1927863.

[43] K. Wei, L. Zhang, Y. Guo, X. Jiang, Health monitoring based on Internet of Medical Things: architecture, enabling technologies, and applications, IEEE Access 8 (2020), https://doi.org/10.1109/ACCESS.2020.2971654.

[44] M. Boumaiz, M. El Ghazi, S. Mazer, M. Fattah, A. Bouayad, M. El Bekkali, Y. Balboul, Energy harvesting based WBANs: EH optimization methods, in: Procedia Comput. Sci., 2019, https://doi.org/10.1016/j.procs.2019.04.147.

[45] M. Cicioğlu, A. Çalhan, SDN-based wireless body area network routing algorithm for healthcare architecture, ETRI J. 41 (2019), https://doi.org/10.4218/etrij.2018-0630.

[46] A.S. Abiodun, M.H. Anisi, M.K. Khan, Cloud-based wireless body area networks: managing data for better health care, IEEE Consum. Electron. Mag. 8 (2019), https://doi.org/10.1109/MCE.2019.2892244.

[47] A.H. Mohd Aman, W.H. Hassan, S. Sameen, Z.S. Attarbashi, M. Alizadeh, L. A. Latiff, IoMT amid COVID-19 pandemic: application, architecture, technology, and security, J. Netw. Comput. Appl. 174 (2021), https://doi.org/10.1016/j.jnca.2020.102886.

[48] R. Hireche, H. Mansouri, A.-S.K. Pathan, Security and privacy management in Internet of Medical Things (IoMT): a synthesis, J. Cybersecur. Priv. 2 (2022), https://doi.org/10.3390/jcp2030033.

[49] B.S Pritika, S. Azam, Risk Assessment of Heterogeneous IoMT Devices: A Review, Technologies, 2023, p. 11, https://doi.org/10.3390/technologies11010031.

[50] J. Srivastava, S. Routray, S. Ahmad, M.M. Waris, Internet of Medical Things (IoMT)-based smart healthcare system: trends and progress, Comput. Intell. Neurosci 2022 (2022), https://doi.org/10.1155/2022/7218113.

[51] A. Ahad, M. Tahir, K.L.A. Yau, 5G-based smart healthcare network: architecture, taxonomy, challenges and future research directions, IEEE Access 7 (2019), https://doi.org/10.1109/ACCESS.2019.2930628.

[52] J. Sengupta, S. Ruj, S.Das Bit, A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT, J. Netw. Comput. Appl. 149 (2020), https://doi.org/10.1016/j.jnca.2019.102481.

[53] M.M. Islam, S. Nooruddin, F. Karray, G. Muhammad, Human activity recognition using tools of convolutional neural networks: a state of the art review, data sets, challenges, and future prospects, Comput. Biol. Med. (2022), 106060.

[54] M.S. Hossain, G. Muhammad, Emotion-aware connected healthcare big data towards 5 G, IEEE Internet Things J. 5 (2018), https://doi.org/10.1109/JIOT.2017.2772959.

[55] T. Hussain, K. Muhammad, S. Khan, A. Ullah, M.Y. Lee, S.W. Baik, Intelligent baby behavior monitoring using embedded vision in IoT for smart healthcare centers, J. Artif. Intell. Syst. 1 (2019), https://doi.org/10.33969/ais.2019.11007.

[56] J.H. Abawajy, M.M. Hassan, Federated Internet of Things and cloud computing pervasive patient health monitoring system, IEEE Commun. Mag. 55 (2017), https://doi.org/10.1109/MCOM.2017.1600374CM.

[57] M.M. Islam, S. Nooruddin, F. Karray, G. Muhammad, Multi-level feature fusion for multimodal human activity recognition in Internet of Healthcare Things, Inf. Fusion. 94 (2023) 17–31.

[58] F. Alam, R. Mehmood, I. Katib, N.N. Albogami, A. Albeshri, Data fusion and IoT for smart ubiquitous environments: a survey, IEEE Access 5 (2017), https://doi.org/10.1109/ACCESS.2017.2697839.

[59] R. Dautov, S. Distefano, R. Buyya, Hierarchical data fusion for smart healthcare, J. Big Data. 6 (2019), https://doi.org/10.1186/s40537-019-0183-6.

[60] M. Chen, J. Yang, J. Zhou, Y. Hao, J. Zhang, C.H. Youn, 5G-smart diabetes: toward personalized diabetes diagnosis with healthcare big data clouds, IEEE Commun. Mag. 56 (2018), https://doi.org/10.1109/MCOM.2018.1700788.

[61] D. Naranjo-Hernández, A. Talaminos-Barroso, J. Reina-Tosina, L.M. Roa, G. Barbarov-Rostan, P. Cejudo-Ramos, E. Márquez-Martín, F. Ortega-Ruiz, Smart vest for respiratory rate monitoring of copd patients based on non-contact capacitive sensing, Sens. (Switzerl.) 18 (2018), https://doi.org/10.3390/s18072144.

[62] H. Zhang, J. Li, B. Wen, Y. Xun, J. Liu, Connecting intelligent things in smart hospitals using NB-IoT, IEEE Internet Things J. 5 (2018), https://doi.org/10.1109/JIOT.2018.2792423.

[63] A. Almas, W. Iqbal, A. Altaf, K. Saleem, S. Mussiraliyeva, M.W. Iqbal, Context-based adaptive fog computing trust solution for time-critical smart healthcare systems, IEEE Internet Things J. (2023), https://doi.org/10.1109/JIOT.2023.3242126.

[64] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, K. Mankodiya, Towards fog-driven IoT eHealth: promises and challenges of IoT in medicine and healthcare, Futur. Gener. Comput. Syst. 78 (2018), https://doi.org/10.1016/j.future.2017.04.036.

[65] P. Pace, G. Aloi, R. Gravina, G. Caliciuri, G. Fortino, A. Liotta, An edge-based architecture to support efficient applications for healthcare industry 4.0, IEEE Trans. Ind. Informat. 15 (2019), https://doi.org/10.1109/TII.2018.2843169.

[66] H. Fouad, A.S. Hassanein, A.M. Soliman, H. Al-Feel, Internet of medical things (IoMT) assisted vertebral tumor prediction using heuristic hock transformation based gautschi model-A numerical approach, IEEE Access 8 (2020) 17299–17309, https://doi.org/10.1109/ACCESS.2020.2966272.

[67] H. Cai, Z. Qu, Z. Li, Y. Zhang, X. Hu, B. Hu, Feature-level fusion approaches based on multimodal EEG data for depression recognition, Inf. Fusion. 59 (2020) 127–138.

[68] M.J. Willemink, W.A. Koszek, C. Hardell, J. Wu, D. Fleischmann, H. Harvey, L. R. Folio, R.M. Summers, D.L. Rubin, M.P. Lungren, Preparing medical imaging data for machine learning, Radiology 295 (2020) 4–15.

[69] M. Illimoottil, D. Ginat, Recent advances in deep learning and medical imaging for head and neck cancer treatment: MRI, CT, and PET scans, Cancer. (Basel) 15 (2023) 3267.

[70] M. Kang, E. Ko, T.B. Mersha, A roadmap for multi-omics data integration using deep learning, Brief. Bioinform. 23 (2022) bbab454.

[71] F. Firouzi, B. Farahani, Architecting IoT Cloud. Intell. Internet Things from Device to Fog Cloud, 2020, https://doi.org/10.1007/978-3-030-30367-9_4.

[72] F. Firouzi, B. Farahani, A. Marinšek, The convergence and interplay of edge, fog, and cloud in the AI-driven Internet of Things (IoT), Inf. Syst. (2021), 101840, https://doi.org/10.1016/J.IS.2021.101840.

[73] I. Martinez, A.S. Hafid, A. Jarray, Design, resource management, and evaluation of fog computing systems: a survey, IEEE Internet Things J. 8 (2021), https://doi.org/10.1109/JIOT.2020.3022699.

[74] A. Yousefpour, C. Fung, T. Nguyen, K. Kadiyala, F. Jalali, A. Niakanlahiji, J. Kong, J.P. Jue, All one needs to know about fog computing and related edge computing paradigms: a complete survey, J. Syst. Archit. 98 (2019) 289–330, https://doi.org/10.1016/j.sysarc.2019.02.009.

[75] M. Aazam, S. Zeadally, K.A. Harras, Offloading in fog computing for IoT: review, enabling technologies, and research opportunities, Futur. Gener. Comput. Syst. 87 (2018), https://doi.org/10.1016/j.future.2018.04.057.

[76] F. Firouzi, S. Jiang, K. Chakrabarty, B. Farahani, M. Daneshmand, J. Song, K. Mankodiya, Fusion of IoT, AI, edge-fog-cloud, and blockchain: challenges, solutions, and a case study in healthcare and medicine, IEEE Internet Things J. 10 (2023), https://doi.org/10.1109/JIOT.2022.3191881.

[77] J. Li, X. Yang, G. Chu, W. Feng, X. Ding, X. Yin, L. Zhang, W. Lv, L. Ma, L. Sun, R. Feng, J. Qin, X. Zhang, C. Gou, Z. Yu, B. Wei, W. Jiao, Y. Wang, L. Luo, H. Yuan, Y. Chang, Q. Cai, S. Wang, P.C. Giulianotti, Q. Dong, H. Niu, Application of improved robot-assisted laparoscopic telesurgery with 5 G technology in urology, Eur. Urol 83 (2023), https://doi.org/10.1016/j.eururo.2022.06.018.

[78] S. Duan, L. Liu, Y. Chen, L. Yang, Y. Zhang, S. Wang, L. Hao, L. Zhang, A 5G-powered robot-assisted teleultrasound diagnostic system in an intensive care unit, Crit. Care 25 (2021), https://doi.org/10.1186/s13054-021-03563-z.

[79] W. Ding, M. Abdel-Basset, H. Hawash, S. Abdel-Razek, C. Liu, Fed-ESD: federated learning for efficient epileptic seizure detection in the fog-assisted internet of medical things, Inf. Sci. (Ny). 630 (2023), https://doi.org/10.1016/j.ins.2023.02.052.

[80] A.K. Idrees, S.K. Idrees, R. Couturier, T. Ali-Yahiya, An edge-fog computing-enabled lossless eeg data compression with epileptic seizure detection in IoMT networks, IEEE Internet Things J. 9 (2022), https://doi.org/10.1109/JIOT.2022.3143704.

[81] S. Hassan, E. Mwangi, P.K. Kihato, IoT based monitoring system for epileptic patients, Heliyon 8 (2022), https://doi.org/10.1016/j.heliyon.2022.e09618.

[82] A. Ahmed, S. Aziz, U. Qidwai, A. Abd-Alrazaq, J. Sheikh, Performance of artificial intelligence models in estimating blood glucose level among diabetic patients using non-invasive wearable device data, Comput. Method. Program. Biomed. Updat. 3 (2023), https://doi.org/10.1016/j.cmpbup.2023.100094.

[83] A. Kumar, K. Sharma, A. Sharma, MEmoR: a Multimodal Emotion Recognition using affective biomarkers for smart prediction of emotional health for people analytics in smart industries, Image Vis. Comput. 123 (2022), https://doi.org/10.1016/j.imavis.2022.104483.

[84] A. Arora, P. Chakraborty, M.P.S. Bhatia, Identifying digital biomarkers in actigraph based sequential motor activity data for assessment of depression: a model evaluating SVM in LSTM extracted feature space, Int. J. Inf. Technol. 15 (2023), https://doi.org/10.1007/s41870-023-01162-5.

[85] M.S. Alauddin, A.S. Baharuddin, M.I.M. Ghazali, The modern and digital transformation of oral health care: a mini review, Healthc 9 (2021), https://doi.org/10.3390/healthcare9020118.

[86] S. Salagare, R. Prasad, Internet of Dental Things (IoDT), intraoral wireless sensors, and teledentistry: a novel model for prevention of dental caries, Wirel. Pers. Commun. 123 (2022), https://doi.org/10.1007/s11277-021-09287-1.

[87] N. Martin, S. Shahrbaf, A. Towers, C. Stokes, C. Storey, Remote clinical consultations in restorative dentistry: a clinical service evaluation study, Br. Dent. J. 228 (2020), https://doi.org/10.1038/s41415-020-1328-x.

[88] Y. Yin, H. Wang, S. Liu, J. Sun, P. Jing, Y. Liu, Internet of Things for diagnosis of Alzheimer's disease: a multimodal machine learning approach based on eye movement features, IEEE Internet Things J. 10, (13), (2023), 11476-11485 10.1109/JIOT.2023.3245067.

[89] H. Gao, L. Zhou, J.Y. Kim, Y. Li, W. Huang, Applying probabilistic model checking to the behavior guidance and abnormality detection for A-MCI patients under wireless sensor network, ACM Trans. Sens. Networks. 19 (2023), https://doi.org/10.1145/3499426.

[90] F. González-Landero, I. García-Magariño, R. Amariglio, R. Lacuesta, Smart cupboard for assessing memory in home environment, Sens. (Switzerl.) 19 (2019), https://doi.org/10.3390/s19112552.

[91] N. Raheja, A. Kumar Manocha, An IoT enabled secured clinical health care framework for diagnosis of heart diseases, Biomed. Signal Process. Control. 80 (2023), https://doi.org/10.1016/j.bspc.2022.104368.

[92] Y.-S. Su, T.-J. Ding, M.-Y. Chen, Deep learning methods in internet of medical things for valvular heart disease screening system, IEEE Internet Things J. 8 (2021) 16921–16932.

[93] Y. Pan, M. Fu, B. Cheng, X. Tao, J. Guo, Enhanced deep learning assisted convolutional neural network for heart disease prediction on the internet of medical things platform, IEEE Access 8 (2020) 189503–189512.

[94] G. Rajkumar, T. Gayathri Devi, A. Srinivasan, Heart disease prediction using IoT based framework and improved deep learning approach: medical application, Med. Eng. Phys. 111 (2023), https://doi.org/10.1016/j.medengphy.2022.103937.

[95] P.R.N. Lalitha, S.V. Jinny, Internet of medical things-based multitiered and hybrid architectural framework for effective heart disease prediction model, Concurr. Comput. Pract. Exp. 34 (2022) e6953.

[96] S. Basak, K. Chatterjee, Smart healthcare surveillance system using IoT and machine learning approaches for heart disease, in: Commun. Comput. Inf. Sci., 2022, https://doi.org/10.1007/978-3-031-23092-9_24.

[97] A. Pati, M. Parhi, M.K. Al Alnabhan, M. Pattanayak, B.K. Habboush, A. K. Nawayseh, An IoT-fog-cloud integrated framework for real-time remote cardiovascular disease diagnosis, Informatics 10 (2023).

[98] S. Shrivastava, T.Q. Trung, N.E. Lee, Recent progress, challenges, and prospects of fully integrated mobile and wearable point-of-care testing systems for self-testing, Chem. Soc. Rev. 49 (2020) 1812–1866, https://doi.org/10.1039/C9CS00319C.

[99] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, M. Imran, Securing IoTs in distributed blockchain: analysis, requirements and open issues, Futur. Gener. Comput. Syst. 100 (2019) 325–343, https://doi.org/10.1016/J.FUTURE.2019.05.023.

[100] M.K. Hasan, S. Islam, R. Sulaiman, S. Khan, A.H.A. Hashim, S. Habib, M. Islam, S. Alyahya, M.M. Ahmed, S. Kamil, M.A. Hassan, Lightweight encryption technique to enhance medical image security on Internet of Medical Things

applications, IEEE Access 9 (2021) 47731–47742, https://doi.org/10.1109/ACCESS.2021.3061710.
[101] A. Avinashiappan, B. Mayilsamy, Internet of Medical Things: security threats, security challenges, and potential solutions, Internet of Thing. (2021) 1–16, https://doi.org/10.1007/978-3-030-63937-2_1/COVER.
[102] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R.U. Rasool, W. Dou, Complementing IoT services through software defined networking and edge computing: a comprehensive survey, IEEE Commun. Surv. Tutorials. 22 (2020) 1761–1804, https://doi.org/10.1109/COMST.2020.2997475.
[103] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, C. Tsatsoulis, Review of security and privacy for the internet of medical things (IoMT): resolving the protection concerns for the novel circular economy bioinformatics, in: Proc. - 15th Annu. Int. Conf. Distrib. Comput. Sens. Syst. DCOSS 2019, 2019, https://doi.org/10.1109/DCOSS.2019.00091.
[104] N. Alsaeed, F. Nadeem, Authentication in the Internet of Medical Things: taxonomy, review, and open issues, Appl. Sci. 12 (2022) 7487, https://doi.org/10.3390/APP12157487.
[105] A. Arfaoui, A. Kribeche, S.M. Senouci, Context-aware anonymous authentication protocols in the internet of things dedicated to e-health applications, Comput. Netw. 159 (2019) 23–36, https://doi.org/10.1016/J.COMNET.2019.04.031.
[106] U. Chatterjee, D. Sadhukhan, S. Ray, An improved authentication and key agreement protocol for smart healthcare system in the context of internet of things using elliptic curve cryptography, Lect. Notes Netw. Syst. 116 (2020) 11–22, https://doi.org/10.1007/978-981-15-3020-3_2/COVER.
[107] G. Xu, F. Wang, M. Zhang, J. Peng, Efficient and provably secure anonymous user authentication scheme for patient monitoring using wireless medical sensor networks, IEEE Access 8 (2020) 47282–47294, https://doi.org/10.1109/ACCESS.2020.2978891.
[108] M.F.A Minahil, K. Mahmood, S. Kumari, A.K. Sangaiah, Lightweight authentication protocol for e-health clouds in IoT-based applications through 5 G technology, Digit. Commun. Netw. 7 (2021) 235–244, https://doi.org/10.1016/J.DCAN.2020.06.003.
[109] S.S. Sahoo, S. Mohanty, B. Majhi, A secure three factor based authentication scheme for health care systems using IoT enabled devices, J. Ambient Intell. Humaniz. Comput. 12 (2021) 1419–1434, https://doi.org/10.1007/S12652-020-02213-6/TABLES/10.
[110] H. Khalid, S.J. Hashim, S.M.S. Ahmad, F. Hashim, M.A. Chaudhary, Cross-SN: a lightweight authentication scheme for a multi-server platform using IoT-based wireless medical sensor network, Electron 10 (2021) 790, https://doi.org/10.3390/ELECTRONICS10070790.
[111] Y. Zhang, R. Gravina, H. Lu, M. Villari, G. Fortino, PEA: parallel electrocardiogram-based authentication for smart healthcare systems, J. Netw. Comput. Appl. 117 (2018) 10–16, https://doi.org/10.1016/J.JNCA.2018.05.007.
[112] M. Fotouhi, M. Bayat, A.K. Das, H.A.N. Far, S.M. Pournaghi, M.A. Doostari, A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT, Comput. Netw. 177 (2020), 107333, https://doi.org/10.1016/J.COMNET.2020.107333.
[113] R. Hajian, S. ZakeriKia, S.H. Erfani, M. Mirabi, SHAPARAK: scalable healthcare authentication protocol with attack-resilience and anonymous key-agreement, Comput. Netw. 183 (2020), 107567, https://doi.org/10.1016/J.COMNET.2020.107567.
[114] A.K. Das, A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks, Peer-to-Peer Netw. Appl. 9 (2016) 223–244, https://doi.org/10.1007/S12083-014-0324-9/TABLES/7.
[115] R. Kumar, R. Tripathi, Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology, J. Supercomput. 77 (2021) 7916–7955, https://doi.org/10.1007/S11227-020-03570-X/TABLES/3.
[116] V. Sureshkumar, R. Amin, V.R. Vijaykumar, S.R. Sekar, Robust secure communication protocol for smart healthcare system with FPGA implementation, Futur. Gener. Comput. Syst. 100 (2019) 938–951, https://doi.org/10.1016/J.FUTURE.2019.05.058.
[117] P. Bhuarya, P. Chandrakar, R. Ali, A. Sharaff, An enhanced authentication scheme for Internet of Things and cloud based on elliptic curve cryptography, Int. J. Commun. Syst. 34 (2021) e4834, https://doi.org/10.1002/DAC.4834.
[118] A.K. Das, A.K. Sutrala, V. Odelu, A. Goswami, A secure smartcard-based anonymous user authentication scheme for healthcare applications using wireless medical sensor networks, Wirel. Pers. Commun. 94 (2017) 1899–1933, https://doi.org/10.1007/S11277-016-3718-6/TABLES/9.
[119] M. Tahir, M. Sardaraz, S. Muhammad, M.S. Khan, A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics, Sustain. 12 (2020) 6960, https://doi.org/10.3390/SU12176960.
[120] F. Wu, X. Li, A.K. Sangaiah, L. Xu, S. Kumari, L. Wu, J. Shen, A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks, Futur. Gener. Comput. Syst. 82 (2018) 727–737, https://doi.org/10.1016/J.FUTURE.2017.08.042.
[121] A. Alrawais, A. Alhothaily, C. Hu, X. Cheng, Fog computing for the Internet of Things: security and privacy issues, IEEE Internet Comput. 21 (2017) 34–42, https://doi.org/10.1109/MIC.2017.37.
[122] I. Makhdoom, M. Abolhasan, J. Lipman, R.P. Liu, W. Ni, Anatomy of threats to the Internet of Things, IEEE Commun. Surv. Tutor. 21 (2019) 1636–1675, https://doi.org/10.1109/COMST.2018.2874978.
[123] C. Camara, P. Peris-Lopez, J.E. Tapiador, Security and privacy issues in implantable medical devices: a comprehensive survey, J. Biomed. Inform. 55 (2015) 272–289, https://doi.org/10.1016/J.JBI.2015.04.007.
[124] R. Xu, Y. Chen, E. Blasch, G. Chen, BlendCAC: a smart contract enabled decentralized capability-based access control mechanism for the IoT, Comput 7 (2018) 39, https://doi.org/10.3390/COMPUTERS7030039.
[125] S. Gusmeroli, S. Piccione, D. Rotondi, A capability-based security approach to manage access control in the Internet of Things, Math. Comput. Model. 58 (2013) 1189–1205, https://doi.org/10.1016/J.MCM.2013.02.006.
[126] S.Y. Lim, P.T. Fotsing, A. Almasri, O. Musa, M.L.M. Kiah, T.F. Ang, R. Ismail, Blockchain technology the identity management and authentication service disruptor: a survey, Int. J. Adv. Sci. Eng. Inf. Technol. 8 (2018) 1735–1745, https://doi.org/10.18517/IJASEIT.8.4-2.6838.
[127] R.M. Aileni, G. Suciu, IoMT: a blockchain perspective, Stud. Big Data. 71 (2020) 199–215, https://doi.org/10.1007/978-3-030-38677-1_9/COVER.
[128] F. Alsubaei, A. Abuhussein, S. Shiva, Security and privacy in the Internet of Medical Things: taxonomy and risk assessment, in: Proc. - 2017 IEEE 42nd Conf. Local Comput. Networks Work. LCN Work, 2017, pp. 112–120, https://doi.org/10.1109/LCN.WORKSHOPS.2017.72, 2017.
[129] O.N. Akande, O.C. Abikoye, A.A. Kayode, O.T. Aro, O.R. Ogundokun, A dynamic round triple data encryption standard cryptographic technique for data security, in: Lect. Notes Comput. Sci. (Including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), 12254 LNCS, 2020, pp. 487–499, https://doi.org/10.1007/978-3-030-58817-5_36/COVER.
[130] T. Li, H. Li, L. Hu, H. Li, A reversible steganography method with statistical features maintained based on the difference value, IEEE Access 8 (2020) 12845–12855, https://doi.org/10.1109/ACCESS.2020.2964830.
[131] J. Ni, K. Zhang, X. Lin, X.S. Shen, Securing fog computing for Internet of Things applications: challenges and solutions, IEEE Commun. Surv. Tutorials. 20 (2018) 601–628, https://doi.org/10.1109/COMST.2017.2762345.
[132] D.R. Raymond, S.F. Midkiff, Denial-of-service in wireless sensor networks: attacks and defenses, IEEE Pervas. Comput. 7 (2008) 74–81, https://doi.org/10.1109/MPRV.2008.6.
[133] T. Borgohain, U. Kumar, S. Sanyal, Survey of Security and Privacy Issues of Internet of Things, 2015.
[134] W. Xu, T. Wood, W. Trappe, Y. Zhang, Channel Surfing and Spatial Retreats, 2004, pp. 80–89, https://doi.org/10.1145/1023646.1023661.
[135] A.D. Wood, J.A. Stankovic, S.H. Son, JAM: a Jammed-area mapping service for sensor networks, in: Proc. - Real-Time Syst. Symp, 2003, pp. 286–297, https://doi.org/10.1109/REAL.2003.1253275.
[136] Y. Xuan, Y. Shen, N.P. Nguyen, M.T. Thai, A trigger identification service for defending reactive jammers in WSN, IEEE Trans. Mob. Comput. 11 (2012) 793–806, https://doi.org/10.1109/TMC.2011.86.
[137] S. Sciancalepore, G. Oligeri, R. Di Pietro, Strength of crowd (SOC)—defeating a reactive jammer in IoT with decoy messages, Sensors 18 (2018) 3492, https://doi.org/10.3390/S18103492.
[138] J. Liu, W. Sun, Smart attacks against intelligent wearables in people-centric Internet of Things, IEEE Commun. Mag. 54 (2016) 44–49, https://doi.org/10.1109/MCOM.2016.1600553CM.
[139] A. Mubashar, K. Asghar, A.R. Javed, M. Rizwan, G. Srivastava, T.R. Gadekallu, D. Wang, M. Shabbir, Storage and Proximity Management for Centralized Personal Health Records Using an IPFS-Based Optimization Algorithm, 31, 2021, https://doi.org/10.1142/S0218126622500104.
[140] X. Nie, A. Zhang, J. Chen, Y. Qu, S. Yu, Blockchain-empowered secure and privacy-preserving health data sharing in edge-based IoMT, Secur. Commun. Networks. 2022 (2022), https://doi.org/10.1155/2022/8293716.
[141] J. Deogirikar, A. Vidhate, Security attacks in IoT: a survey, in: Proc. Int. Conf. IoT Soc. Mobile, Anal. Cloud, I-SMAC 2017, 2017, pp. 32–37, https://doi.org/10.1109/I-SMAC.2017.8058363.
[142] H. Ning, H. Liu, L.T. Yang, Cyberentity security in the internet of things, Comput. (Long. Beach. Calif 46 (2013) 46–53, https://doi.org/10.1109/MC.2013.74.
[143] M. Seliem, K. Elgazzar, BIoMT: blockchain for the internet of medical things, in: 2019 IEEE Int. Black Sea Conf. Commun. Networking, BlackSeaCom 2019, 2019, https://doi.org/10.1109/BLACKSEACOM.2019.8812784.
[144] M. Mettler, Blockchain technology in healthcare: the revolution starts here, in: 2016 IEEE 18th Int. Conf. e-Health Networking, Appl. Serv. Heal, 2016, https://doi.org/10.1109/HEALTHCOM.2016.7749510, 2016.
[145] R.M.P.H.K. Rathnayake, M.S. Karunarathne, N.S. Nafi, M.A. Gregory, Cloud Enabled Solution for Privacy Concerns in Internet of Medical Things, in: 2018 28th Int. Telecommun. Networks Appl. Conf. ITNAC 2018, 2019, https://doi.org/10.1109/ATNAC.2018.8615361.
[146] A. Lounis, A. Hadjidj, A. Bouabdallah, Y. Challal, Secure and scalable cloud-based architecture for e-Health wireless sensor networks, in: 2012 21st Int. Conf. Comput. Commun, Networks, 2012, https://doi.org/10.1109/ICCCN.2012.6289252.
[147] K. Lorincz, D.J. Malan, T.R.F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, S. Moulton, Sensor networks for emergency response: challenges and opportunities, IEEE Pervas. Comput. 3 (2004) 16–23, https://doi.org/10.1109/MPRV.2004.18.
[148] J.P.A. Yaacoub, M. Noura, H.N. Noura, O. Salman, E. Yaacoub, R. Couturier, A. Chehab, Securing internet of medical things systems: limitations, issues and recommendations, Futur. Gener. Comput. Syst. 105 (2020), https://doi.org/10.1016/j.future.2019.12.028.
[149] S. Ibrokhimov, K.L. Hui, A.A. Al-Absi, M. Sain, Multi-factor authentication in cyber physical system: a state of art survey, in: 2019 21st Int. Conf. Adv. Commun. Technol., IEEE, 2019, pp. 279–284.