Computer Systems Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2024.049026

REVIEW

IoMT-Based Healthcare Systems: A Review

Tahir Abbas[1,*], Ali Haider Khan[2], Khadija Kanwal[3], Ali Daud[4,*], Muhammad Irfan[5], Amal Bukhari[6] and Riad Alharbey[6]

[1]Department of Computer Science, TIMES Institute, Multan, 60000, Pakistan

[2]Department of Software Engineering, Faculty of Computer Science, Lahore Garrison University, Lahore, 54000, Pakistan

[3]Institute of Computer Science and Information Technology (CS&IT), The Women University, Multan, 60000, Pakistan

[4]Faculty of Resilience, Rabdan Academy, Abu Dhabi, 22401, United Arab Emirates

[5]School of Computer Science, National College of Business Administration & Economics, Multan, 54000, Pakistan

[6]Department of Information Systems and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah, 21959, Saudi Arabia

*Corresponding Authors: Tahir Abbas. Email: drtahirabbas@t.edu.pk; Ali Daud. Email: alimsdb@gmail.com

Received: 25 December 2023 Accepted: 04 March 2024 Published: 17 July 2024

ABSTRACT

The integration of the Internet of Medical Things (IoMT) and the Internet of Things (IoT), which has revolutionized patient care through features like remote critical care and real-time therapy, is examined in this study in response to the changing healthcare landscape. Even with these improvements, security threats are associated with the increased connectivity of medical equipment, which calls for a thorough assessment. With a primary focus on addressing security and performance enhancement challenges, the research classifies current IoT communication devices, examines their applications in IoMT, and investigates important aspects of IoMT devices in healthcare. The evaluation extends so far as to examine an IoMT-based system in the healthcare space, highlighting limitations in Industry 5.0 and healthcare institutions. IoMT devices are systematically categorized according to how well they can strengthen infrastructures; this process exposes operational flaws, gaps in the literature, and real-world risks. The importance of this research is in its thorough analysis of the security and operational facets of IoMT devices, with the explicit objective of promoting secure and efficient medical practices.

KEYWORDS

Internet of things (IoT); internet of medical things (IoMT); communication technology; information security; machine learning; Healthcare Industry 5.0

1 Introduction

Internet of Things (IoT) devices are widely used in several businesses, particularly in the healthcare sector, serving as a permanent solution to various problems. User-friendly wireless communication technology over the internet is the main reason for accepting and deploying these Internet of Things-based devices in many fields. These days, physical items with sensors, processor power, software, and

other systems and devices connected to the internet or other communication networks and devices are referred to as "Internet of Things" (IoT) things. This new method has been highly beneficial to the healthcare industry. These gadgets are made and referred to as the "Internet of Medical Things" (IoMT) in the healthcare industry. These devices are capable of data acquisition and transmission in the healthcare department to facilitate the experts in medicine for the well-being of humans.

Healthcare IT is connected via a network of physical infrastructure, software applications, and internet-connected medical devices, which are known as the Internet of Medical Things (IoMT). These devices allow the system to connect to the remote, wireless devices securely to the internet for rapid and flexible data processing of medical sciences. The effect of the Internet of Things on the medical healthcare business is apparent and long-lasting. This is predicted that the IoMT globally in 2017, increased from $41 to $158 billion by 2022 [1], according to a recent Deloitte poll. IoMT is primarily concerned with healthcare and medical applications. IoMT requires a more robust information security infrastructure than other Internet of Things (IoT) systems due to the complex rules and the sensitivity around healthcare data.

An IoT paradigm makes real-world applications with a scalable and service-based architecture possible. Because the IoT can be accessed from anywhere, supports a variety of service and computing paradigms, and reacts quickly to demands, its design is advantageous for real-world applications [2]. Sensors such as smartwatches, digital headbands, creative electrodes, and sensor patches have been developed to meet this crucial need for healthcare [3]. First, a heterogeneous IoT platform transmits data from WS devices to a healthcare facility for analysis. With the right app and a smartphone, one may view and interact with WS data. An IoT communication protocol supports device-to-device and device-to-an IoT modes of communication technologies.

An IoT has a chance to show what it can achieve because of the requirement for administration and control to reduce physical touch, as studied [4]. Isolation zones benefit from the employment of remote temperatures, drone-mounted sensors, robots that suppress epidemics, and triggered door sensors. For example, an IoMT monitors a patient's medical records from afar, even if they are thousands of kilometers apart. Medical records keep track of long-term health issues. mHealth devices can be used to locate sick people and transport them to hospitals [5]. Those responsible for the patient's treatment can access data from these mobile health gadgets. A patient's vital signs can be monitored via dashboards and sensors incorporated into hospital beds in the future. In the future, global health will be more important than environmental conditions. Medical robots are predicted to be replaced by personal fitness trackers by 2022, and their value is estimated at $160 billion.

It is critical to classify the existing IoT connectivity technologies effectively utilized in IoMT systems in order to maximize security and healthcare performance. This classification has to be more precise, considering things like security procedures, verification methods, interoperability guidelines, data transfer effectiveness, scalability, compatibility with various devices, resistance to online attacks, and adherence to medical standards. While classifying technologies based on efficiency and interoperability improves overall healthcare performance, grouping them based on strong security characteristics guarantees the protection of critical healthcare data. IoMT systems are more resilient when scalability, device compatibility, and resilience to cyber threats are considered. Furthermore, they are maintaining adherence to healthcare regulations. A thorough classification approach considers the special needs and difficulties IoMT applications face, promoting a safe and effective healthcare system.

Various security issues arise when Internet of Things (IoT) technology is integrated into healthcare services, especially regarding the Internet of Medical Things (IoMT) architecture [6]. To avoid unwanted access and data breaches, the main priority is protecting patient data's privacy and

confidentiality in the face of widespread device connectivity. IoT devices have built-in vulnerabilities that make them vulnerable to various cyber threats, from ransomware assaults to malware, highlighting the vital need for robust security features. Interoperability issues arise because disparate devices cannot have uniform security protocols, which could jeopardize the integrity of the healthcare system as a whole. Network security becomes critical when sensitive medical data is sent between IoMT systems to prevent unwanted access and data manipulation. Ensuring that only authorized individuals have access to essential healthcare data is a challenging endeavor that requires careful management of user identities and access control. The regulatory landscape is made more difficult by the need to comply with laws, especially those pertaining to healthcare, like HIPAA. The alarming frequency of IoT-related data breaches in healthcare institutions is shown by recent studies, underscoring the critical necessity for all-encompassing cybersecurity solutions. A multidimensional strategy is needed to address these issues, including implementing sophisticated cybersecurity measures, industry-wide industry collaboration for standardization, and regulatory framework adherence to promote a secure IoMT ecosystem.

In healthcare systems, integrating medical equipment interconnected across multiple network layers might provide several vulnerabilities. This increased attack surface presents serious security issues, with a wide range of devices interacting via local networks, cloud services, and the wider internet. Malicious actors can access devices through vulnerabilities, ranging from out-of-date software to inadequate authentication procedures. To address these vulnerabilities, it is imperative to develop rigorous access control and authentication methods, ensure secure data transmission, and update software regularly. By separating vital medical equipment, network segmentation improves security and lessens the impact of a possible compromise. Proactive responses are made possible by early threat identification offered by intrusion detection systems and anomaly detection. A thorough security strategy must include employee knowledge and training, especially concerning cybersecurity best practices.

Moreover, compliance with regulatory standards creates a foundation for protecting patient information and applying robust security protocols throughout networked medical devices. Simply put, mitigating these possible vulnerabilities necessitates a multipronged strategy integrating technological fixes, procedural safety measures, and regulatory compliance. Internet of Things (IoT) devices have become indispensable in several industries, most notably healthcare, providing long-lasting answers to chronic problems. The ease of use of IoT-based devices' wireless internet connectivity technology is a significant factor in their broad adoption. IoT refers to a large category of physical products with sensors, software, computing power, and other embedded components. These objects can be accessed via the internet or other communication networks. This revolutionary technology is known as the healthcare industry's IoMT. Despite the impressive progress in IoMT, several issues remain in the current environment. Careful thought must be given to issues like data security, interoperability, and the efficient integration of IoT devices into existing healthcare frameworks. Healthcare data confidentiality and sensitivity present serious problems that call for practical solutions to protect patient data. Ensuring smooth communication and data sharing is further complicated by the heterogeneity of IoMT devices and the absence of defined protocols. Novel methods and strategies are needed to address these problems. Suggested algorithms and frameworks are essential for overcoming obstacles and improving IoMT's general effectiveness in the healthcare industry. These advanced solutions seek to strengthen data security and privacy safeguards in the IoMT ecosystem by utilizing machine learning algorithms, decentralized processing, and sophisticated encryption techniques.

Additionally, adopting interoperability standards and defined communication protocols can facilitate the integration of various IoMT devices, promoting a more unified and effective healthcare ecosystem. Within this framework, our research explores the ever-changing field of IoMT-based healthcare systems, looking at current problems and suggesting new algorithms and methods to solve them. By offering perspectives on the revolutionary potential of IoMT and emphasizing the usefulness of proposed algorithms, our work aims to further the ongoing discussion about improving the security, interoperability, and general efficacy of IoMT in healthcare.

The article focuses on IoT-based remote healthcare monitoring, smart hospitals, ingestible sensor tracking, and improving chronic disease treatment [6]. The ability to carry out ordinary work while patients are under continuous health monitoring is the key advantage of the Internet of medical Things-based remote healthcare monetarization, as it is the benefit of lower hospital expenditures. With the advancement in security protection [7], strategies, and the new forms of assaults targeting the IoMT system, a thorough examination of current IoMT security techniques and threats is studied. As a result, this article examines current information security and attack approaches for IoMT systems. A DeepFM with IoMT-based illness prediction [8,9] is presented in this paper. DeepFM is used to predict the occurrence of hepatitis based on structured disease data. It makes a few improvements and parameter adjustments to make it a more in line solution in actual learning situations.

This study considers stress analysis [10] using integrated edge devices linked to IoMT. They created "Stress-Lysis", an IoMT system that can also detect the stress levels of the patients or persons (at the edge) while the data is stored on the cloud. The designed methodology of stress lysis can be implemented into a glove or wristband to track the stress levels in instantaneous time duration. The general purpose was to plan or design a smart and intelligent system that aids and guides in preserving the emotional equilibrium of the users by providing solutions so that a person's stress level can be monitored.

The authentication of the Internet of Medical Things system monitors pressure ulcer prevention [11] in hospitals, as proposed in this work. This study looked at how well healthcare workers in the intensive care unit adhered to the changes in dependent patients' positions to cure the establishment of pressure ulcers. This study has comprehensively reviewed COVID-19, the role of drones, the Internet of Things, artificial intelligence systems, 5G, and blockchain technologies [12,13], and their applications. The intense increase in COVID-19 events around the globe has highlighted the need for immediate steps to prevent the epidemic from becoming catastrophic.

Clients and patients have more options when it comes to healthcare, and the digital healthcare system is becoming more and more well-liked [14]. Because of digital health care, there has been a consistent increase in health applications. IoMT is a cutting-edge digital health system that uses a large variety of biological sensors and enhanced cloud and wireless network capabilities. There is a 33% decrease in security risk, a 52% reduction in latency, and a 42% reduction in execution cost when comparing BECSAF to prior healthcare IoMT studies. The internet is progressively dominated by smartphones and other mobile devices [15]; from social media to the Internet of Things, applications are freely available, can be loaded on mobile devices and servers, and are used by many businesses. In a new concept called mobile edge computing (MEC), tasks can be transferred from mobile devices to other devices to save energy. However, all of the current research focuses on portable power. When offloading and scheduling in the MEC network, compute node resources and application deadlines are frequently overlooked. It has been found that a mobile edge cloud (mob-cloud) architecture may meet deadlines while using little energy at each node. In this study, linear integer programming and

convex optimization are used to try to solve the convex optimization problem. The mob cloud uses a variety of virtual computers to do edge computing.

The DEETS algorithm framework, which uses deadlines and the energy economy to organize jobs, is discussed in this article. This paradigm prioritizes tasks, resources are sought, and mobility is considered while developing plans. Additionally, DEETS balances the quantity of energy utilized and the time required to complete a task. According to computer simulations, the suggested DEETS is 50% more efficient than any present approach regarding application time and energy consumption. The growing number of digital healthcare applications [16] incorporate Internet of Medical Things (IoMT) platforms that can train using machine learning algorithms. Machine learning is heavily used by IoMT devices to ensure that resources such as time and energy are utilized simultaneously.

The classification of IoT connectivity technologies within IoMT systems is a complex procedure requiring careful evaluation of several criteria. The most crucial factor is how strong the security measures are, which include authentication procedures, encryption techniques, and resistance to online attacks. Interoperability standards are essential because they mandate that technologies follow pre-established communication protocols. Scalability, adaptability, and efficient data transfer enable technologies to adjust to healthcare situations dynamically. Device compatibility becomes essential, necessitating the seamless integration of technology with various medical devices. The classification is further shaped by the products' cost-effectiveness, usability, dependability, resistance to cyberattacks, and adherence to healthcare regulations. Ethical and legal issues, including privacy concerns must also guide the classification process. This comprehensive strategy aims to provide a well-informed classification framework that will enable the effective implementation of IoMT systems in healthcare environments by considering security, performance, and ethical factors.

Developing or modifying communication protocols for connected medical devices within the Internet of Medical Things (IoMT) brings several complex issues and subtle considerations. Medical equipment is diverse by nature, highlighting the need for protocols that can handle a range of data formats and communication needs. Standardized and widely acknowledged methods are necessary to guarantee flawless interoperability. One of the main challenges is finding a careful balance between reliable security measures and rapid real-time communication. This means protocols must be durable and efficient in protecting sensitive healthcare data. Developing protocols becomes more challenging when it comes to meeting the particular limitations of medical contexts, such as dependability and low latency needs. It is essential to incorporate strong security mechanisms, such as authentication and encryption, to defend against cyberattacks. To ensure compliance and maintain ethical data handling methods, considerations must include matching the new or modified processes with current healthcare standards and regulations. Essentially, the difficulty is in developing communication protocols that combine adaptability, security, and customized functionality to satisfy the complex needs of connected medical devices in the Internet of Medical Things (IoMT) ecosystem.

The study looks into a wide range of IoT communication devices, each contributing differently to strengthening the IoMT infrastructure in the healthcare industry. These gadgets include wearables and Internet of Things (IoT) devices used in intelligent medicine. They connect to form a network that enables real-time data retrieval from multiple sources, such as hospitals and patient perspectives. In conjunction with these devices, the study explores the critical function of edge and fog computing, providing a dispersed data gathering and transmission system. By supplying continuous, real-time health information, wearables, and IoT devices support the IoMT architecture and allow intelligent healthcare systems to make quick judgments. This network of connections guarantees that doctors may remotely access vital patient data, enabling quick decision-making for better patient care. In

addition to improving healthcare services by seamlessly integrating patient data into the decision-making process, the study highlights the value of these devices in building a responsive and efficient IoMT infrastructure.

The research strategically groups the IoMT devices available to support IoMT infrastructures, meet particular requirements, and maximize system performance. Each device is categorized according to its function, role, and contribution to the IoMT ecosystem. Wearables and IoT devices, for instance, are classified according to how they contribute to ongoing patient monitoring and data gathering. Due to their essential function in establishing a dispersed network for data processing and transmission, edge and fog computing nodes are grouped. The research also explores the classification of blockchain-enabled devices, highlighting their function in offering a decentralized and safe archiving mechanism. A more detailed understanding of how various IoMT device types jointly strengthen the IoMT infrastructure is made possible by this systematic categorization. By classifying them according to their functionality, the study offers valuable insights into the distinct and crucial roles that different device categories play in constructing a resilient and interconnected healthcare system. This classification lays the groundwork for additional investigation, permitting a thorough examination of how IoMT devices improve healthcare infrastructure.

The summary of the most common devices used in healthcare organizations is represented in Table 1. The details of abbreviations used in Table 1 are precisely explained in Table 2.

Table 1: Recent public IoMT devices with their categories

PM	MT	HC	Ambient	AD
Motion S	Infusion pump	MRI	Identification D	Coordinators
BG D	ICPS	X-rays	Gyroscope S	Network D
BP D	CRM	SR	Motion S	End-User D
Temperature S	SMC	PU SR	Vibration S	DB Services
Pulse oximetry			Monitoring D	
Pacemakers			Alarm D	
EEG S			ID C	
ECG S				
RR S				
MA S				
Implantable D				
Pill-Line S				
Aggregators				

Table 2: Detail and description of abbreviations

Abbreviation	Description
PM: Physiological monitoring	This stands for monitoring vital signs, blood pressure, and other physiological parameters.
MT: Medical treatment	Denotes the range of medical procedures and therapies given to patients.

(Continued)

Table 2 (continued)

Abbreviation	Description
HC: Hospital connected	Defines systems or gadgets that are networked together in a medical setting.
AD: Additional devices	Additional Devices are devices utilized in addition to the leading medical equipment.
CRM: Heart rhythm management	This pertains to controlling heart rhythms, frequently associated with using pacemakers or comparable apparatuses.
S: Sensors	Indicates tools or parts that are in charge of identifying and quantifying physical characteristics.
D: Device	A general word for a technological or medical tool utilized for a particular function.
BP: Blood pressure	It is the force that flowing blood applies to blood vessel walls.
BG: Blood glucose	This refers to the blood's glucose content and is crucial for managing diabetes.
DB: Database	This is a systematic collection of data arranged for simple handling and retrieval.
RR: Respiratory rate	It shows how many breaths are taken in a minute.
MA: Muscle activity	This refers to the tracking or measurement of the activity and contractions of the muscles.
SR: Surgical robotics	Discusses the application of robotic devices during medical operations.
SMC: Smart medical capsules	This term describes intelligent capsules used in medicine, frequently for medicinal or diagnostic purposes.
PU SR: Prosthetic using surgical robots	This course covers the application or development of prosthetic devices through the lens of surgical robots.
IDC: Implantable device charger	Provides information about a charger system that guarantees the continuing operation of implanted medical devices.

The summary of data acquisition methods & data sources for making a dataset from different papers is explained in Table 3.

Table 3: The Summary of data acquisition methods and data source

Paper	Acquisition method	Data sources
[2]	WS (Wearable Sensor) data inputs/Sources	Many devices are gathered through 8 organizational units and are distributed to the different healthcare centers.
[5]	Electrocardiogram sensor, electromyogram sensor, blood pressure sensor	Real-time, health care center

(Continued)

Table 3 (continued)

Paper	Acquisition method	Data sources
[6]	51 patients confirmed COVID-19	MSC-COVID-19 data was collected from Wuhan City, China.
[17]	Medical sensors compute physiological and electrical signals ECG, EEG, etc.)	Devices by sensor
[18]	Multimodal data, INTERFACE	SEED data set and DEAP database
[19]	Heart and disease	UCI repository, heart disease dataset https://archive.ics.uci.edu/ml/datasets/ (accessed on 10/02/2024)
[20]	CICIDS2017	Global Dataset
[21]	Online fuzzy based trust management (FTM) nodes data	Cooja simulation environment
[22]	Glucose data	Material Research Centre (MRC), MNIT-Jaipur, MNIT SMDP-C2SD
[23]	Real-time data	Data collected from battery-powered IoT sensors
[24]	Sleeping data in an analog single	By using a Bluetooth device
[25]	Datasets of COVID-19 from different countries that contain symptoms are observed in 316,800 patients.	Information was gathered from clinics, medical foundations, and worldwide that are coronavirus disease victims of COVID-19 time. The side effects and the symptoms in the dataset incorporate internal heart level, circulatory strain, heartbeat, etc. This shows the convincing outcomes of patients having COVID-19 in their bodies.
[26]	Three different kinds of datasets were considered, consisting of Alzheimer's disease images, brain, lung, and breast cancer images.	Only different sources to collect the dataset
[27]	The public dataset and the bus drive monitoring dataset	Edge computing-based mask identification (EC-Mask) via online cameras in the buses
[28]	ISIC, HAM10000, PADUFES HAMI0000 dataset	The dataset consists of different kinds of skin lesions and thermoscopic images.
[29]	Dataset for heart disease	UCI open-source heart disease dataset
[30]	Dataset for heart disease	UCI, an open-source heart disease dataset
[31]	CIFAR-10-LT dataset	EHR for high speed computing
[32]	Lung and colon cancer histopathological image dataset (LC25000)	Github online
[33]	Lung cancer dataset	Kaggle online data repository

The following are the paper's significant contributions in this direction:

- Healthcare scalability importance and challenges.
- An exhaustive literature review on IoMT-based healthcare systems is provided.
- Discussion about literature review for IoMT-based healthcare systems.
- Insights about the healthcare industry's research challenges, limitations, and future direction.

The primary purpose of this literature review is to provide a complete overview of the IoMT-based healthcare system and the numerous medical devices that make up the healthcare ecosystem. The literature contains (a) the various generic IoMT architectures used; (b) the categories of the medical devices used in the medical environment; (c) the summary of the proposed methodology, algorithms, and the results of different studies. We structure the rest of the paper as follows. Section 2 includes the importance and challenges of healthcare scalability. Section 3 describes the literature review. Section 4 elaborately explains the Key Aspects of IoMT with Healthcare Industry 5.0. Section 5 presents open research challenges, limitations, and future direction of the Healthcare Industry 5.0. Finally, Section 6 concludes the paper with an idea of future work.

2 Healthcare Scalability Importance and Challenges

Scalability in healthcare services, which involves the process of patient prioritizing and analysis, is a problematic undertaking [31]. The demand for healthcare services is gradually increasing as the number of patients grows due to population growth. The priority of healthcare services is determined by the severity of the patient's condition.

The study carefully examines how the IoMT devices can be integrated with the fundamental ideas of Industry 5.0, focusing on how these devices can be used in healthcare settings. It clarifies the critical role that IoMT devices play in enabling real-time data analysis, promoting wise decision-making and creating smooth communication between healthcare providers and institutions. Furthermore, the study highlights the role edge and fog computing play in healthcare data's distributed and decentralized processing. This aligns with the fundamental ideas of Industry 5.0, which emphasizes the value of distributed intelligence and self-governing operational frameworks.

Finding advanced research aids for the facility of accurate and efficient healthcare systems is both significant and problematic [31]. Several bioinformatics studies are being conducted to improve the organizational process and solve challenges in healthcare facilities [31–33]. This area offers pertinent works searching for why the number of elderly patients who require quick and effective telemedicine services is increasing. The increase in patients is expected in the face of an aged population [34] and calamities [14]. There are several complications with healthcare services, but the most serious is the aging population [35].

The study explores the main features of IoMT devices widely used in the healthcare industry, illuminating their critical function in improving remote patient care and facilitating real-time therapy. Wearables and Internet of Things (IoT) devices become essential elements that enable ongoing patient monitoring and data gathering. These gadgets operate along with edge and fog computing systems to create an intelligent healthcare network that easily transfers real-time health data. As these IoMT devices give healthcare providers quick access to vital health indicators, they play a significant role in facilitating remote patient care by allowing them to monitor patients from a distance. The study focuses on improving the efficiency of diagnosis and treatment decisions by integrating these devices into the healthcare infrastructure. Additionally, the use of IoMT devices contributes to the paradigm change in intelligent medicine, where prompt access to patient data guarantees quick and well-informed

decision-making, ultimately enhancing the standard of care for patients receiving remote therapy and facilitating real-time interventions.

The healthcare system is facing several complications, and as a result, significant demographic changes have occurred [33]. The social and economic burdens increase, leading to severe difficulties and long-term challenges in healthcare [36]. Globally, burdened healthcare systems and societies may contribute to population aging issues. By 2030, 13% of the world's population will be over 65, significantly damaging the healthcare system [36]. Chest cancer, brain tumors, diabetes, lung cancer, heart failure, and hypertension are only a few of the severe disorders that have a direct effect on the cost of medical health care all over the globe [37]. To provide quality service, physically handling illness is difficult for the global healthcare system [34]. The increase in patients in the healthcare domain also increases the cost of healthcare services in the United States (US). According to the Medicaid Services (CMS) and Centers for Medicare, US healthcare [38] spending rises year after year and in future predictions (2012–2028) as illustrated in Fig. 1.

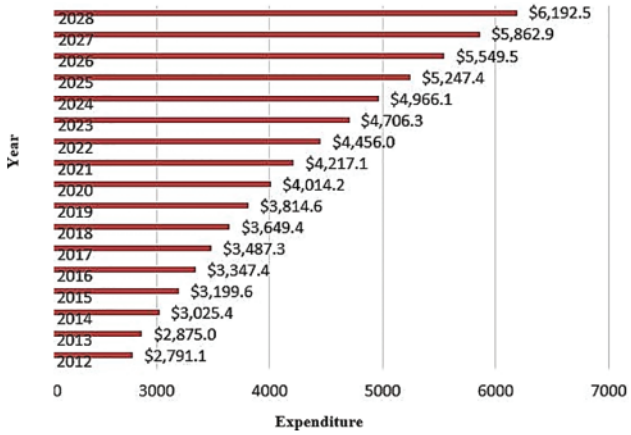

Figure 1: NH expenditure (Billons $) in the US

An intelligent framework that integrates several technologies to improve healthcare services is what an IoMT-based system means in healthcare. The system comprises a network of wearables, IoT, and medical devices connected and managed by edge and fog computing platforms. Its main goal is to make data interchange and communication between various devices easier, enabling real-time monitoring and healthcare decision-making. The system built on IoMT offers a wide range of features and services. First, it makes it possible for wearables and Internet of Things devices to monitor patients continuously, giving medical experts immediate access to critical health data.

Furthermore, the system facilitates remote patient care by enabling medical professionals to make well-informed judgments based on real-time data, even when they are far away. The IoMT-based system demonstrates adaptability in meeting different healthcare needs by helping with disease prediction, stress management, and secure data transmission. Moreover, it is essential to Industry 5.0, which emphasizes using smart technology to transform healthcare procedures. The IoMT-based system's specified functions and services enhance patient outcomes, expedite medical procedures, and create a more adaptable and effective healthcare ecosystem.

The study uncovers a number of IoMT device constraints in healthcare organizations, all of which affect how effective IoMT-based healthcare systems are overall. One significant drawback is that IoMT devices are not interoperable, which makes it challenging to integrate and communicate data across

platforms. This restriction impairs the development of a cohesive and thorough patient health profile, which impacts the effectiveness of the procedures involved in diagnosis and therapy. Moreover, security issues provide a major barrier because IoMT equipment could be vulnerable to hacker attacks and illegal access. The confidentiality and privacy of patient data could be jeopardized, which directly affects the reliability of IoMT systems. A cohesive and secure network cannot be developed if IoMT device communication protocols are not sufficiently standardized, which makes security issues worse. The analysis also notes that there are limits to the scalability of IoMT implementations since it may be difficult for healthcare organizations to integrate an increasing number of devices, which could result in system overload and inefficiencies. Furthermore, healthcare organizations may face financial challenges due to the high upfront costs of obtaining and deploying IoMT devices, which would restrict their widespread adoption.

IoMT has a revolutionary function in the context of Industry 5.0, which emphasizes the integration of human intelligence with cyber-physical systems. It creates an intelligent healthcare ecosystem by establishing a complex network of wearables, IoT technology, and medical devices.

The IoMT allows data to be collected and transmitted in real-time, giving medical personnel quick access to vital patient information. This helps achieve Industry 5.0's objective of improving the responsiveness and efficiency of healthcare processes. The smooth communication and collaboration made possible by the interconnection of medical devices through IoMT fosters a more integrated and flexible healthcare system. Furthermore, IoMT advances Industry 5.0's notion of patient-centered, customized treatment. They optimize patient outcomes through customized healthcare treatments made possible by ongoing monitoring and data-driven insights. Industry 5.0's emphasis on human-machine collaboration—where technology augments and enhances the capabilities of healthcare professionals—aligns with the integration of smart technologies through IoMT.

The potential of IoMT to establish a networked and intelligent healthcare ecosystem that emphasizes productivity, customization, and teamwork to redefine and improve patient care standards is essentially what makes IoMT's contribution to Industry 5.0 in healthcare settings.

3 Literature Review

The digital transformation [39] and Industrial Revolution 4.0 greatly impacted the Healthcare Industry 4.0. In this revolution, the healthcare industry groomed a lot for the well-being of humans. Healthcare on demand [40] also contributes a lot to the automated Healthcare Industry 4.0.

For monitoring physiological data such as ECG, EEG, blood pressure, and temperature [41], the IoT-based systems consist of a large number of sensor nodes that use modern technologies such as Wi-Fi and Bluetooth. Second, modern cloud, social media, IoT, and e-healthcare systems [42] must now secure their users' privacy. Pictures and medical information about patients are often included in health and medical records. Patients' privacy should be protected by not disclosing this type of information.

The ecosystem constantly expands and integrates software, hardware, physical items, and computational devices [43,44], so they may talk to one another and collect data. An IoT allows users to connect with real and virtual things, including personalized healthcare domains, through a single platform that is accessible to all. Increasing numbers of older persons with chronic conditions that require remote monitoring, the desire for telemedicine, rising medical expenditures, and emergent nations make the IoT an essential topic in healthcare systems. The Internet of Things, centered on preventive and predictive care in the new era of health care, is the focus (p2Health) [45]. Behavior and

environmental factors, as well as physiological and psychiatric factors, are the most significant aspects of healthcare.

An IoT, or the An IoT, is an innovative new approach to linking devices from several industries together over the internet [46]. Modern healthcare is one of the most intriguing submissions of the IoT. As a result, doctors, nurses, and hospital beds require healthcare monitoring systems. This paper demonstrates the wearable sensor and the compact patch for measuring things like the PPG, ECG, and body temperature. This suggested sensor patch can be utilized to constantly estimate blood pressure based on the arrival time of the pulse, eliminating the requirement for additional cables and devices. To collect and analyze data, the sensor patch includes the main board, a battery charger, and three sensors for monitoring vital signs.

Connecting devices from diverse fields via the internet via the IoT is proposed in this paper. An IoT has several intriguing applications in modern healthcare. As a result, doctors, nurses, and hospital beds require healthcare monitoring systems. IoT is a new way of linking devices from various fields over the internet [47] proposed in this paper. The IoT has several intriguing applications in modern healthcare. As a result, the traditional healthcare system needs additional doctors, nurses, hospital beds, and health monitoring systems.

The way healthcare is given is evolving in the Internet of Things era [48]. There are many opportunities to improve in terms of quality, safety, and efficiency regarding the IoT-based system in healthcare scenarios. Additionally, there are promising scientific, economic, and social opportunities. Nevertheless, security concerns are associated with this connection, such as a data breach triggered by malware that steals the logging details. A hack on a patient's medical gadget could also expose their private information to the public. IoT devices are ubiquitous, and healthcare-based IoT is especially critical; therefore, today's computing world is concerned with security.

For e-healthcare, blockchain technologies and the internet of Things (IOT) [49] are increasingly explicit. It is possible to obtain real-time patient data in health care by using the Internet of Things and the Internet of Medical Things devices. This study examines the Internet of Things (IoT) in the healthcare system [50]. This is partly due to the growing importance of IoT applications in healthcare. There have been efforts to improve monitoring in the IoT-based medical healthcare system. This study examines how IoT and cloud architecture work together. Accuracy and power consumption are major issues for the Internet of Things. Researchers are improving IoT-based healthcare solutions. The study also examines how to manage cloud-based IoT healthcare data. The Internet of Things in health care systems was also examined for its advantages and disadvantages. The majority of research investigations are successful in identifying a wide range of symptoms and accurately predicting disease. It becomes more convenient to monitor the health concerns of elderly persons when using an IoT-based healthcare system. Having so many gadgets makes them easier to break into, but they take a lot of energy and don't have the means to do so.

The IoT in Healthcare refers to the digitalization of data [51], particularly health data, and it is becoming increasingly common in healthcare. During the COVID-19 situation, the exponential rise of IoT in healthcare took a dramatic turn. A confluence of rapidly evolving technologies is reshaping ioT in healthcare. In addition, there are issues with data protection, the digital divide, government and other stakeholders, and the behavior of doctors and hospitals when making and delivering healthcare technology. There is an in-depth look at IoT in healthcare, including how different factors influence its current condition and how it is being used in various countries worldwide. In addition, it proposes regulatory changes for an ideal IoT healthcare pathway in India.

Patients, their medical data, and the connections to and from their medical devices must be kept safe and secure as IoT advances in healthcare [52]. The privacy and security of mobile applications are jeopardized when their codes are modified or reverse-engineered. This could lead to severe consequences. There has been a rapid increase in the adoption of IoMT workflow applications [53]. You may run these web-based apps in this scheme, combined with mobile computing with edge and cloud technology. Divesting and development are essential in a distributed network. Biomedical systems use IoT-based biomedical applications [54], such as healthcare or telecare, prevention, diagnosis, therapy, and monitoring. The idea of the Internet of Things needs to comprise wireless body area networks (WBANs) (IoT) and radio frequency identification (RFID). WBANs and RFID technologies are used in this project to create a new IoT healthcare framework for hospital information systems. To model and simulate the proposed framework, Riverbed Modeler software has been employed. The ISO/IEEE 110 QoS criteria for latency and data rate are met using the suggested energy-aware system. It is also demonstrated that the suggested framework can easily be done by following some case studies using hospital information systems and creating a simulation environment that saves time.

This new technology, known as IoT, is a result of how quickly items are becoming connected to the internet. However, IoT necessitates a new network architecture to keep pace with its rapid expansion. The IoT is applied to an extensive range of industries, and healthcare departments. People who receive healthcare, as well as those who work in healthcare facilities, benefit from the use of IoT.

Adding sensors and gadgets [55] relevant to healthcare to the Internet of Things has transformed the IoMT. An investment in IoMT will allow us to better satisfy the needs of our patients promptly. Especially following COVID's impact on the world, it is gradually replacing traditional healthcare systems. This information may be useful in directing future investigations in this area. More than any other network item, medical devices in IoT-based healthcare are more likely to be attacked or targeted by security risks [56,57]. A portion of patient data can currently be protected during transmission, but sophisticated attacks and threats, such as collusion attacks or data leaking, are not prevented.

Security and integrity of clinical or medical information have become significant issues for applications that deliver medical healthcare facilities due to the progression of the IoT in the field [58,59]. A hybrid security is proposed in this research to ensure the safety of diagnostic text data in medical photographs. 2D-DWT-2L steganography 2-D discrete wavelet transform level 1 techniques can be combined with a proposed hybrid encryption strategy technique to create the model. The proposed hybrid encryption scheme includes Rivest, Shamir, and Adleman algorithms. Encryption of the secret data is the first step in the suggested model. To hide the outcome, it employs 2D-DWT-1L or 2D-DWT-2L. People use grayscale and color graphics as cover image to hide variable amounts of text. MSE (Mean Square Error), SC (Structural Content), PSNR (peak signal-to-noise ratio), BER, and correlation are used to estimate the given system's performance. There was a wide variation in the PSNR values for color and grayscale images: 50.59 to 57.44, and 50.52 to 56.09. The MSE values for the color photos and the MSE values for the grayscale images were between 0.12 and 0.57, respectively. Images with BER values of zero and SSIM, SC, and correlation values of 1 were compared. Confidential patient data can be hidden in cover images with high invisibility, low degradation, and capacity of the given stego-image using the suggested methodology.

IoT has various advantages in healthcare, such as the ability to examine patients closely and analyze the data obtained from the examination [60,61]. Blood pressure cuffs, Glucose meters, and other devices that capture data about a patient's vital signs are at the forefront of IoT and medical device integration. This paper mainly studies the significance of the Internet of Things in healthcare, its vulnerabilities, assaults, and security issues, and how to fix them. This study is divided into two sections.

Patients can be watched and treated in real-time from a distance using an IoMT, which integrates IoT technology and healthcare facilities [62].

When utilizing a hybrid model of blended filtering algorithms, the suggested ProTrip system operates effectively [63]. The food suggestion mechanism of an Internet of Things-based healthcare assistance system is being tested. We also present a thorough case study on the potential application of dietary recommendations for health management. The proposed method is more accurate and efficient than existing techniques on a real-time dataset. Healthcare professionals increasingly use technology, such as patient portals, to connect with their patients [64], even when they are not physically there. Even though an increasing number of doctors are turning to patient portals to improve service quality and save costs, relatively few patients are taking advantage of this new technology. The author presented a transfer learning-based IoMT-based healthcare model in [65] that monitors senior citizens' health and provides them with service-oriented emergency responses in case of a medical emergency. The aging of the global population threatens conventional healthcare models that depend on in-person health monitoring. When tracking senior citizens' health, the suggested model performs better using TL approaches than the Artificial Neural Network technique, which achieves a 93.6% accuracy rate. The author [66] provided a unique scoring-aided FL framework that selects mobile clients with better transmission circumstances and more tailed data to upload their local models using a scoring-based sampling technique. In particular, they used the logits to investigate data distribution among local clients and provide a scoring technique for client selection based on logits to mitigate the effects of long-tailed data.

Additionally, it addressed the effects of severe fading by introducing a unique logits and model upload rate-based client selection technique and integrating the channel state information (CSI) and data rate of clients into the logits-based score. The outcomes of the experiments show how successful our suggested framework is. For instance, the suggested framework provided accuracy increases ranging from 4.44% to 28.36% compared to the traditional FedAvg. The author in [67] suggested a secure IoMT-based method and transfer learning has been considered. In the smart Healthcare Industry 5.0, precise disease prediction is achieved using the Google Net Deep Machine-Learning Model. Using the safe IoMT-based transfer learning approach, they predicted the deadly cancer disease in the human body.

Additionally, the cancer disease prediction in the smart healthcare sector is validated using the outcomes of the suggested secure IoMT-based transfer learning approach. In the smart Healthcare Industry 5.0, they suggested a secure IoMT-based transfer learning methodology that achieved cancer disease prediction with a score of 98.8%. In [68], the author proposed an intelligent system for lung disease diagnosis that considers federated deep extreme learning combined with edge computing. In the suggested intelligent system, federated deep extreme machine learning forecasts lung disease. Additionally, a fused weighted deep extreme machine learning methodology is applied to improve lung disease prediction to reinforce the suggested model. The suggested fused weighted federated deep extreme machine learning strategy produced a 97.2% accuracy. A summary of healthcare systems is provided in the following Table 4.

Table 4: Summary of healthcare systems

Authors	Method/Technique used in the paper	Proposed idea & preprocessing methodology	Tools	Evaluation
[2]	Classification learning, sigmoid function analysis	(CDP-UA) Cognitive data processing for uncertainty analysis to improve and manage the effectiveness of WS data, to diagnose the diseases	Unknown	Unknown
[5]	Fog computing, wireless resources	(FogC-IoMT) fog based computing-based IoMT is used to minimize the optimization in healthcare monitoring	Unknown	Unknown
[17]	BRLE algorithm	Decentralized Energy Efficient Model, adaptive energy efficient (EEA) algorithm	MATLAB	Unknown
[3]	Edge-IoMT	Internet of Medical Things is basically used to telecommunicate remotely with the capacity and idleness of streamline transmission for quick decision process management in a virtual environment.	Unknown	Wearable IoMT-based eye examination device
[4]	K-means, filtered, density, and K-means, farthest clustering, filtering, and density algorithms	By using machine learning algorithms prediction and diagnosis of diseases can be made	MATLAB	The Hoeffding Tree algorithm gives more than 92% accuracy Random Forest algorithm gives more than 93% accuracy,
[18]	CNN, LRN, logistic sigmoid, and tanh sigmoid	Motion-aware and intelligent IoMT system, robust tracking model	Unknown	Accuracy 95%
[19]	CNN, Deep learning	Convolutional neural network is assessed by the enhanced deep learning	Unknown	The precision of up to 99.1%.
[65]	Federated learning (FL), fog and edge computing	An important role of the FL-based system within an IoMT to combat the COVID-19 pandemic, Knowledge Discovery from Data	Unknown	Unknown
[20]	DNN	Federated transfer learning based intrusion detection system (IDS) is preferably used to secure the devices that are mainly connected to the patient's healthcare system	Unknown	CICIDS2017-Tues 95.14 CICIDS2017-Wed 62.50 CICIDS2017-Thur 88.25
[21]	IoMT infrastructures	Fuzzy logic processing, fuzzy filters, fuzzy based trust management to avoid the Sybil attack on the IOMT	Unknown	Unknown
[66]	Federated learning, edge cloudlet computing	AD models are used in federated learning that is run on the cloud to prevent the patient data from being shared	Unknown	Unknown
[67]	Stress calculation on live and sudden fluctuation by using daily, weekly, and monthly physiological fluctuations during stress.	iFeliz a stress control system	Unknown	Unknown

(Continued)

Table 4 (continued)

Authors	Method/Technique used in the paper	Proposed idea & preprocessing methodology	Tools	Evaluation
[22]	Deep Neural Network (DNN), sigmoid activation for DNN	Glucose measurement (CGM) to control diabetes	Unknown	The value of the regression coefficient is obtained as 0.81
[23]	Neural network radial basis function	A remote healthcare tracking system known as the RGFNN technique is used to detect the patient's location	Unknown	Rigorous simulations
[24]	Star topology Bluetooth network to fuse data of sleep-aware applications, CNN for sleep events detection.	SDFN is a data fusion network for IOT-enabled devices.	Unknown	The model shows that they lessen jam issues in the data and help to regain the battery power of IOT devices
[25]	An IoT and machine learning, OpenCV	A systematic approach to fight against the COVID-19 disease, preprocessing with panadas libraries	Unknown	Model evaluation in real-time
[26]	Data executed in the cloud platform, validation accuracy of 85%	Unknown	Unknown	Unknown
[27]	Deep learning (DL) for categorization of alzheimer's disease images, brain, lungs, and breast cancer	(OCS) Opposition-based crow search algorithm, efficient medical image classification L-Classifier model is used for feature selection	MATLAB	Accuracy 95%
[28]	Deep learning and VR	The measures for public health care (ECMask) edge computing-based mask identification framework is used	Unknown	Accuracy 97.98%
[68]	Wireless body area network technology (WBANT) for observing a patient's condition, channel state information, signal strength indication	A framework or system design for the identification of narcolepsy disease combining wireless communication technology and computer science analytics	Unknown	A framework evaluated 10 humans indoors
[69]	An IoT	Stress-Lysis to alleviate the stress issues	Unknown	Accuracy was as high as 99.7%
[29]	Photoplethysmography via the smartphone camera	Android application that counts the oxygen saturation levels (also called SPO2) and the heart rate of COVID-19 patients	Unknown	Accuracy 97%
[30]	Levy flight algorithm	MSSO-ANFIS prediction model	Unknown	Precision is 96.54
[70]	Scoring-aided Federated Learning framework	Wireless IoMT based healthcare system	Unknown	Unknown

(Continued)

Table 4 (continued)

Authors	Method/Technique used in the paper	Proposed idea & preprocessing methodology	Tools	Evaluation
[71]	Transfer learning	IoMT-based healthcare model that monitors senior citizens' health	Unknown	Accuracy 93.6%
[72]	Transfer learning	Secure IoMT for disease prediction	MATLAB	Accuracy 98.8%
[73]	Fused weighted federated deep extreme machine learning	Lung cancer disease prediction model for Healthcare 5.0	MATLAB	Accuracy 97.2%
[74]	Generic framework for patient physiological parameters (PPPs) privacy and security in S-CI	Towards smart healthcare: Patient data privacy and security in sensor-cloud infrastructure	Unknown	Unknown
[75]	DBP-DeepCNN	Prediction of DNA-binding Proteins using Wavelet-based Denoising and Deep Learning	Python	Produced 6.92% and 1.32% higher accuracy
[76]	Deep learning	Improving prediction of growth hormone-binding Proteins	Python	88.09% and 83.33%
[77]	An innovative blockchain-based access control model (BBACM)	A blockchain-based system for patient data privacy and security	Unknown	Unknown

4 Key Aspects of IoMT with Healthcare Industry 5.0

This particular section explores the more intricate aspects of an IoMT patient monitoring system that functions within the larger context of Healthcare Industry 5.0. Our thorough evaluation study presents a novel way to integrate cloud services, IoMT, and IoT devices with edge and fog computing, imagining an intelligent healthcare system powered by smart medicine. Wearables and Internet of Things (IoT) gadgets enable this revolutionary technology to provide smooth communications between patients and healthcare facilities. This system's primary function is real-time data retrieval from various sources, such as hospitals and patient perspectives. This fog and distributed edge computing system orchestrates this dynamic data collection procedure. Therefore, medical professionals can make prompt and informed judgments from the comfort of their homes thanks to the effective transmission of the collected data. This greatly enhances patient treatment outcomes while also expediting decision-making.

A crucial component of our research is incorporating edge and fog computing, acknowledged as essential in guaranteeing patient safety in smart healthcare. This article looks into these vital elements in response to the demand for a more in-depth analysis. It examines important facets of IoMT within the changing context of the global Healthcare Industry 5.0. We next continue our analysis to the creation of a dispersed network enabled by edge computing nodes and IoMT. We also present the network-wide integration of blockchain technology, which provides a distributed, decentralized, and secure archiving mechanism. This cutting-edge solution includes a transaction record caching method that greatly improves the security of healthcare data, something that previous research has frequently ignored.

Through the integration of private edge computing nodes, an important but sometimes overlooked feature in the literature now under publication, an extra layer of security is investigated. These nodes are essential to bolster healthcare data's security and privacy, making the system stronger and more resilient. In this investigation, we provide Federated Learning (FL) as a novel approach to solve important privacy and security concerns related to healthcare data. This innovative method revolutionizes standard machine learning by enabling collaborative model training across dispersed devices or servers, such as those within multiple hospitals. With FL, just the local model weights are shared instead of sending raw patient data to a central cloud server. Since each hospital uses its dataset for local model training, confidential patient data is kept inside the walls of the individual healthcare facility. Subsequently, the common local model weights are transmitted to a cloud-based master model that combines insights from several hospitals without requiring direct access to unprocessed patient data. This decentralized coordination protects the privacy of individual patient records while optimizing the model's performance as a whole. Hospitals manage and maintain control over their data locally, greatly improving data security and privacy.

Furthermore, because FL transmits just the smaller model weights, it reduces the requirement for large bandwidth. In addition to making it easier to create extremely accurate illness prediction models, collaborative model training in FL allows for intelligent disease detection based on various datasets without violating patient privacy. All things considered, FL is a paradigm leap in machine learning for the healthcare industry, offering a strong solution that gives security and privacy in processing medical data a top priority.

5 Open Research Challenges, Limitations, and Future Direction of the Health Care Industry 5.0

The medical healthcare situation in different countries across the world is fairly unique. The other perspectives are that there are progressive devices for medical, skilled specialists in medicine, well-maintained, well-equipped hospitals and clinics, and increasing medical expenditures. The elderly population is trying to adjust to this kind of complex system. By considering all these problems, the people whose lives depend on how effectively and efficiently these healthcare firms manage the healthcare problems and eliminate the differences to provide them good medical care. The first need is to identify the issues healthcare industries face because of the diversity of perceptions. The nine different types of issues are observed in the healthcare industry. The following are the challenges that the healthcare departments face: (1) Harnessing advanced medical devices, (2) Integrated healthcare services, (3) Cyber security, (4) Rising healthcare costs, (5) Investment in IoMT healthcare, (6) Healthcare regulatory changes, (7) Pressure on pharmaceutical prices, (8) Opioid crisis, (9) Healthcare staffing shortages.

In the digitalization of healthcare, the volume of medical information is expected to double every 73 days by 2020, according to estimates by the Global Future Council. More than 318,000 health apps are now accessible on top app stores worldwide (up from only two years ago), with more than 200 new health apps being uploaded daily. A system biology approach to disease prevention, surveillance, early detection, and intervention will be possible thanks to data integration. The rapid advancement of science and medicine has greatly aided in human well-being. Exciting advances in science and medicine, such as precision medicine, immunotherapy, microbiology, genetic engineering, and regenerative medicine, have been made in recent years. Some other advanced technological evolutions leveraged in health and healthcare, like big data and analytics, AI, nanotechnologies, virtual and augmented reality, and modern machinery, are all examples of technological advancements used in health and healthcare (robotics, drones, 3D printing).

With an emphasis on practical security issues, the report identifies significant research and operational gaps in the current state of IoMT-based healthcare systems. One considerable research gap concerns the lack of established protocols and norms for the security of IoMT and calls for the creation of globally recognized standards to provide reliable and uniform security measures over a range of IoMT implementations. Operational shortcomings also draw attention to the lack of transparency in reporting processes and datasets, which impedes a thorough assessment of security measures. Another significant research gap is the lack of investigation into explainable AI models in healthcare applications, which is crucial for improving algorithm interpretability and addressing security issues. There are operational gaps in IoMT systems that call for a closer look at privacy concerns and ethical issues about patient data. The report also emphasizes the need for practical security threat assessments tailored to IoMT-based healthcare systems to achieve a sophisticated awareness of vulnerabilities and take preventative action to lessen new threats. It is essential to close these gaps if safe and appropriate IoMT deployment in healthcare is to proceed.

The study offers suggestions for closing the operational and research gaps found in next IoMT-based healthcare system advances. In order to overcome the deficiency of standardization in IoMT security protocols, the research suggests that scholars, practitioners, and policymakers work together to create widely recognized standards. This would establish a foundation for reliable and consistent security measures. To improve transparency, the study recommends that the IoMT research community establish uniform reporting requirements, providing clearer documentation of datasets and techniques. It suggests investigating explainable AI models for use in healthcare applications to overcome the low interpretability of IoMT algorithms. The study recommends addressing security concerns and promoting trust among healthcare practitioners by implementing AI models that are more open and interpretable. Ethical concerns and privacy issues can be lessened by thoroughly examining these facets of IoMT systems, and appropriate deployment procedures can be created. It also suggests carrying out thorough security threat analyses tailored to IoMT-based healthcare systems. This entails taking proactive steps to find and fix such weaknesses so that strong protection against new attacks is maintained. Overall, the suggestions are meant to direct IoMT advancements in the future and promote the safe, open, and morally upright development of healthcare systems.

In the future, we need to handle all the healthcare industry challenges for the betterment of human beings. The harmony between the advanced IoMT devices and healthcare systems is also important. To overcome cybersecurity, the latest advanced infrastructures for the Healthcare Industry 5.0 are needed to tackle this issue. Advanced machine learning models should be implemented for the diagnosis of diseases. For healthcare data security and privacy purposes, Federated learning and private edge technology should be adopted.

6 Conclusion

This comprehensive analysis of IoMT-based healthcare system studies has yielded insightful information about the ever-evolving and promising field of medical technology. Convolutional neural networks (CNNs) and deep learning algorithms, in particular, showed impressive accuracy of up to 99.1%, highlighting their usefulness in healthcare applications. The real-world benefits of IoMT applications, including as stress reduction, illness prediction, and safe data transfer, highlight how revolutionary this technology may be in improving medical procedures. However, the main source of difficulties for the research is the lack of transparency in the datasets and reporting procedures. This constraint makes it more difficult to evaluate the studies thoroughly and emphasizes how important it is for the IoMT research community to standardize reporting procedures. Going forward,

cooperation between scholars, practitioners, and policymakers is essential to improve the validity and repeatability of IoMT research. The analyzed research shows that IoMT can potentially transform healthcare practices regarding practical benefits. In real-world applications, implementing Edge Cloudlet Computing, Federated Learning, and Fog Computing for pandemic response and patient data protection demonstrates the flexibility and instant utility of IoMT systems. The research does have several limitations, though. The lack of transparency surrounding methodology and datasets has been noted as a prevalent concern across studies, impeding a comprehensive evaluation of their robustness and generalizability. This restriction highlights the necessity of standardizing reporting procedures in IoMT research to guarantee comparability, reproducibility, and clarity.

Anticipating the future and resolving the noted constraints ought to be top priorities for IoMT research. Initially, a coordinated endeavor to create uniform reporting protocols throughout the IoMT research community will enhance transparency and enable significant cross-study comparisons. Furthermore, investigating how explainable AI models might be included in healthcare applications could improve the understandability of IoMT algorithms, encouraging higher confidence and uptake among medical professionals. In addition, it is crucial to look at the ethical issues related to patient data security and privacy in IoMT systems to guarantee their responsible and fair implementation in healthcare environments.

In conclusion, even if IoMT-based healthcare systems have a lot of potential, achieving their full potential will need overcoming current obstacles and responsibly and transparently advancing research. The recommended paths for future study are intended to tackle these issues and support the creation of strong, dependable, and morally sound IoMT applications in the healthcare industry.

Acknowledgement: We thank our families and colleagues who provided us with moral support.

Funding Statement: This project is funded by UJ-02-032-DR funding provided by University of Jeddah, Jeddah, Saudi Arabia.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Tahir Abbas, Ali Daud, and Khadija Kanwal; data collection: Tahir Abbas, Khadija Kanwal, and Amal Bukhari; analysis and interpretation of results: Tahir Abbas, Muhammad Irfan, and Ali Haider Khan; draft manuscript preparation: Tahir Abbas, Muhammad Irfan, and Khadija Kanwal; supervision: Ali Haider Khan, Ali Daud, and Riad Alharbey. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The authors declare that all data supporting the findings of this study are available within the article and publicly accessible.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] P. Wal, A. Wal, N. Verma, R. Karunakakaran, and A. Kapoor, "Internet of medical things–the future of healthcare," *Open Public Health J.*, vol. 15, no. 1, 2022.

[2] G. Manogaran, M. Alazab, H. Song, and N. Kumar, "CDP-UA: Cognitive data processing method wearable sensor data uncertainty analysis in the internet of things assisted smart medical healthcare systems," *IEEE J. Biomed. Health Inform.*, vol. 25, no. 10, pp. 3691–3699, Oct. 2021. doi: 10.1109/JBHI.2021.3051288.

[3] Ç. Dilibal, "Development of Edge-IoMT computing architecture for smart healthcare monitoring platform," in *Proc. 2020 4th Int. Symp. Multidiscip. Studies Innov. Technol. (ISMSIT)*, Istanbul, Turkey, 22–24 Oct., 2020.
[4] E. Elbasi and A. I. Zreikat, "Efficient early prediction and diagnosis of diseases using machine learning algorithms for IoMT data," in *IEEE World AI IoT Cong. (AIIoT)*, Seattle, WA, USA, 2021.
[5] Y. Qiu, H. Zhang, and K. Long, "Computation offloading and wireless resource management for healthcare monitoring in fog-computing-based internet of medical things," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15875–15883, Nov. 2021. doi: 10.1109/JIOT.2021.3066604.
[6] K. Qian *et al.*, "Computer audition for fighting the SARS-CoV-2 corona crisis—Introducing the multitask speech corpus for COVID-19," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 16035–16046, 1 Nov. 2021. doi: 10.1109/JIOT.2021.3067605.
[7] S. Vishnu, S. R. J. Ramson, and R. Jegan, "Internet of medical things (IoMT)–An overview," in *Proc. 2020 5th Int. Conf. Dev. Circ. Syst. (ICDCS)*, Coimbatore, India, 2020. doi: 10.1109/ICDCS48716.2020.243558.
[8] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali and R. Jain, "Recent advances in the internet-of-medical-things (IoMT) systems security," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 8707–8718, Jun. 2021. doi: 10.1109/JIOT.2020.3045653.
[9] Z. Yu, S. U. Amin, M. Alhussein, and Z. Lv, "Research on disease prediction based on improved deepFM and IoMT," *IEEE Access*, vol. 9, pp. 39043–39054, Feb. 2021. doi: 10.1109/ACCESS.2021.3062687.
[10] L. Rachakonda, S. P. Mohanty, E. Kougianos, and P. Sundaravadivel, "Stress-Lysis: A DNN-integrated edge device for stress level detection in the IoMT," *IEEE Trans. Consum. Electron.*, vol. 65, no. 4, pp. 474–483, Nov. 2019. doi: 10.1109/TCE.2019.2940472.
[11] J. Sarmiento-Rojas, P. A. Aya-Parra, J. M. P. Sayo, L. F. C. Torres, and O. L. C. Ferreira, "Validation of an IoMT-based monitoring system for pressure ulcer prevention in a hospital environment: A pilot," in *Proc. 2021 IEEE 2nd Int. Cong. Biomed. Eng. Bioeng. (CI-IB&BI)*, Bogota D.C., Colombia, Oct. 13–15, 2021. doi: 10.1109/CI-IBBI54220.2021.9626058.
[12] V. Chamola, V. Hassija, V. Gupta, and M. Guizani, "A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact," *IEEE Access*, vol. 8, pp. 90225–90265, May 2020. doi: 10.1109/ACCESS.2020.2992341.
[13] I. Ud Din, A. Almogren, M. Guizani, and M. Zuair, "A decade of internet of things: Analysis in the light of healthcare applications," *IEEE Access*, vol. 7, pp. 89967–89979, Jul. 2019. doi: 10.1109/ACCESS.2019.2927082.
[14] A. Lakhan *et al.*, "Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 664–672, Feb. 2023. doi: 10.1109/JBHI.2022.3165945.
[15] A. Lakhan, M. A. Mohammed, A. N. Rashid, S. Kadry, and K. H. Abdulkareem, "Deadline aware and energy-efficient scheduling algorithm for fine-grained tasks in mobile edge computing," *Int. J. Web Grid Serv.*, vol. 18, no. 2, pp. 168–193, Feb. 2022. doi: 10.1504/IJWGS.2022.121935.
[16] A. Lakhan, M. A. Mohammed, M. Elhoseny, M. D. Alshehri, and K. H. Abdulkareem, "Blockchain multi-objective optimization approach-enabled secure and cost-efficient scheduling for the internet of medical things (IoMT) in fog-cloud system," *Soft Comput.*, vol. 26, no. 13, pp. 6429–6442, May 2022. doi: 10.1007/s00500-022-07167-9.
[17] A. H. Sodhro *et al.*, "Decentralized energy efficient model for data transmission in iot-based healthcare system," in *Proc. IEEE 93rd VTC2021-Spring*, Helsinki, Finland, Apr. 25–28, 2021.
[18] T. Zhang, M. Liu, T. Yuan, and N. Al-Nabhan, "Emotion-aware and intelligent internet of medical things toward emotion recognition during COVID-19 pandemic," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 16002–16013, Nov. 2021. doi: 10.1109/JIOT.2020.3038631.
[19] Y. Pan, M. Fu, B. Cheng, X. Tao, and J. Guo, "Enhanced deep learning assisted convolutional neural network for heart disease prediction on the internet of medical things platform," *IEEE Access*, vol. 8, pp. 189503–189512, Sep. 2020. doi: 10.1109/ACCESS.2020.3026214.

[20] Y. Otoum, Y. Wan, and A. Nayak, "Federated transfer learning-based ids for the internet of medical things (IoMT)," in *Proc. GC Wkshps*, Madrid, Spain, 2021.
[21] A. Almogren, I. Mohiuddin, I. U. Din, H. Almajed, and N. Guizani, "FTM-IoMT: Fuzzy-based trust management for preventing Sybil attacks in internet of medical things," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4485–4497, Mar. 2021. doi: 10.1109/JIOT.2020.3027440.
[22] A. M. Joshi, P. Jain, and S. P. Mohanty, "iGLU: Non-invasive device for continuous glucose measurement with IoMT framework," in *Proc. IEEE Comput. Soc. Annual Symp. VLSI (ISVLSI)*, Limassol, Cyprus, 2020.
[23] S. K. S. Tyagi, P. Goswami, S. R. Pokhrel, and A. Mukherjee, "Internet of things for healthcare: An intelligent and energy efficient position detection algorithm," *IEEE Trans. Ind. Inform.*, vol. 18, no. 8, pp. 5458–5465, Aug. 2022. doi: 10.1109/TII.2021.3110963.
[24] F. Yang *et al.*, "Internet-of-things-enabled data fusion method for sleep healthcare applications," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15892–15905, Nov. 2021. doi: 10.1109/JIOT.2021.3067905.
[25] M. M. S. Choyon, M. Rahman, M. M. Kabir, and M. F. Mridha, "IoT based health monitoring & automated predictive system to confront COVID-19," presented at 2020 IEEE 17th Int. Conf. HONET, Charlotte, NC, USA, 2020.
[26] R. J. S. Raj, S. J. Shobana, I. V. Pustokhina, D. A. Pustokhin, D. Gupta and K. Shankar, "Optimal feature selection-based medical image classification using deep learning model in internet of medical things," *IEEE Access*, vol. 8, pp. 58006–58017, Mar. 2020. doi: 10.1109/ACCESS.2020.2981337.
[27] X. Kong *et al.*, "Real-time mask identification for COVID-19: An edge-computing-based deep learning framework," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15929–15938, Nov. 2021. doi: 10.1109/JIOT.2021.3051844.
[28] P. R. Medi, P. Nemani, V. R. Pitta, V. Udutalapally, D. Das and S. P. Mohanty, "SkinAid: A GAN-based automatic skin lesion monitoring method for IoMT frameworks," presented at 19th Int. Conf. OCIT, Bhubaneswar, India, 2021.
[29] M. A. Khan and F. Algarni, "A healthcare monitoring system for the diagnosis of heart disease in the IoMT cloud environment using MSSO-ANFIS," *IEEE Access*, vol. 8, pp. 122259–122269, Jul. 2020. doi: 10.1109/ACCESS.2020.3006424.
[30] X. Yuan, J. Chen, K. Zhang, Y. Wu, and T. Yang, "A stable AI-based binary and multiple class heart disease prediction model for IoMT," *IEEE Trans. Ind. Inform.*, vol. 18, no. 3, pp. 2032–2040, Mar. 2022. doi: 10.1109/TII.2021.3098306.
[31] H. O. Alanazi, A. A. Zaidan, B. B. Zaidan, M. L. M. Kiah, and S. H. Al-Bakri, "Meeting the security requirements of electronic medical records in the ERA of high-speed computing," *J. Med. Syst.*, vol. 39, no. 1, pp. e30, Dec. 2014. doi: 10.1007/s10916-014-0165-3.
[32] A. A. Zaidan, B. B. Zaidan, Z. Kadhem, M. Larbani, M. B. Lakulu and M. Hashim, "Challenges, alternatives, and paths to sustainability: Better public health promotion using social networking pages as key tools," *J. Med. Syst.*, vol. 39, no. 2, pp. e16, Jan. 2015. doi: 10.1007/s10916-015-0201-y.
[33] B. B. Zaidan, A. Haiqi, A. A. Zaidan, M. Abdulnabi, M. L. M. Kiah and H. A. Muzamel, "Security framework for nationwide health information exchange based on telehealth strategy," *J. Med. Syst.*, vol. 39, no. 5, pp. 1–19, 2015. doi: 10.1007/s10916-015-0235-1.
[34] N. Kalid *et al.*, "Based on real time remote health monitoring systems: A new approach for prioritization "large scales data" patients with chronic heart diseases using body sensors and communication technology," *J. Med. Syst.*, vol. 42, no. 4, pp. 2184, Mar. 2018. doi: 10.1007/s10916-018-0916-7.
[35] J. Culley, E. Svendsen, J. Craig, and A. Tavakoli, "A validation study of 5 triage systems using data from the 2005 Graniteville, South Carolina, chlorine spill," *J. Emerg. Nurs.*, vol. 40, no. 5, pp. 453–460, Sep. 2014. doi: 10.1016/j.jen.2014.04.020.
[36] J. Sun, Y. Guo, X. Wang, and Z. Qiang, "MHealth for aging China: Opportunities and challenges," *Aging Dis.*, vol. 07, no. 1, pp. 53–67, Jan. 2016. doi: 10.14336/AD.2015.1011.
[37] R. Sparks, B. Celler, C. Okugami, R. Jayasena, and M. Varnfield, "Telehealth monitoring of patients in the community," *J. Intell. Syst.*, vol. 25, no. 1, pp. 37–53, Jan. 2015. doi: 10.1515/jisys-2014-0123.

[38] "National Health Expenditure (NHE) Fact Sheet | CMS," Accessed: Jun. 09, 2022. [Online]. Available: https://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/NHE-Fact-Sheet
[39] M. Ćwiklicki, M. Duplaga, and J. Klich, "The digital transformation of Healthcare Health 4.0," Routledge International Studies in Health Economics 2022. Accessed: Dec. 10, 2023. [Online]. Available: https://api.pageplace.de/preview/DT0400.9781000514933_A42211221/preview-9781000514933_A42211221.pdf
[40] A. Gleiss, "The patient will see you now–Towards an understanding of on-demand healthcare," in *Proc. CBI*, Antwerp, Belgium, Jun. 22–24, 2020, pp. 154–161. doi: 10.1109/CBI49978.2020.00024.
[41] H. Magsi, A. H. Sodhro, M. S. Al-Rakhami, N. Zahid, S. Pirbhulal and L. Wang, "A novel adaptive battery-aware algorithm for data transmission in IoT-based healthcare applications," *Electronics*, vol. 10, no. 4, pp. 367, 2021. doi: 10.3390/electronics10040367.
[42] R. Hamza, Z. Yan, K. Muhammad, P. Bellavista, and F. Titouna, "A privacy-preserving cryptosystem for IoT E-healthcare," *Inf. Sci.*, vol. 527, no. 4–6, pp. 493–510, Jul. 2020. doi: 10.1016/j.ins.2019.01.070.
[43] M. H. Kashani, M. Madanipour, M. Nikravan, M. P.Asghari, and E. Mahdipour, "A systematic review of IoT in healthcare: Applications, techniques, and trends," *J. Netw. Comput. Appl.*, vol. 192, no. 5, pp. 103164, Oct. 2021. doi: 10.1016/j.jnca.2021.103164.
[44] T. A. Rashid, C. Chakraborty, and K. Fraser, *Advances in Telemedicine for Health Monitoring: Technologies, Design, and Applications*. UK: Institution of Engineering and Technology, Jul. 2020.
[45] M. Haghi *et al.*, "A flexible and pervasive IoT-based healthcare platform for physiological and environmental parameters monitoring," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5628–5647, Jun. 2020. doi: 10.1109/JIOT.2020.2980432.
[46] J. Li *et al.*, "A secured framework for SDN-based edge computing in iot-enabled healthcare system," *IEEE Access*, vol. 8, pp. 135479–135490, Jul. 2020. doi: 10.1109/ACCESS.2020.3011503.
[47] X. C. Yin, Z. G. Liu, B. Ndibanje, L. Nkenyereye and S. M. Riazul Islam, "An Iot-based anonymous function for security and privacy in healthcare sensor networks," *Sensors*, vol. 19, no. 14, pp. 3146, Jul. 2019. doi: 10.3390/s19143146.
[48] I. M. B. Filho, G. Aquino, R. S. Malaquias, G. Girao and S. R. M. Melo, "An IoT-based healthcare platform for patients in ICU beds during the COVID-19 outbreak," *IEEE Access*, vol. 9, pp. 27262–27277, Feb. 2021. doi: 10.1109/ACCESS.2021.3058448.
[49] P. P. Ray, D. Dash, K. Salah, and N. Kumar, "Blockchain for IoT-based healthcare: Background, consensus, platforms, and use cases," *IEEE Syst. J.*, vol. 15, no. 1, pp. 85–94, Mar. 2021. doi: 10.1109/JSYST.2020.2963840.
[50] S. Selvaraj and S. Sundaravaradhan, "Challenges and opportunities in iot healthcare systems: A systematic review," *SN Appl. Sci.*, vol. 2, no. 1, pp. 641, Dec. 2019. doi: 10.1007/s42452-019-1925-y.
[51] S. P. Dash, "The impact of IoT in healthcare: Global technological change & the roadmap to a networked architecture in India," *J. Indian Inst Sci.*, vol. 100, no. 4, pp. 773–785, Nov. 2020. doi: 10.1007/s41745-020-00208-y.
[52] F. Nausheen and S. H. Begum, "Healthcare IoT: Benefits, vulnerabilities and solutions," presented at 2018 2nd Int. Conf. ICISC, Coimbatore, India, 2018.
[53] A. Lakhan *et al.*, "Hybrid workload enabled and secure healthcare monitoring sensing framework in distributed fog-cloud network," *Electronics*, vol. 10, no. 16, pp. 1974, 2021. doi: 10.3390/electronics10161974.
[54] F. Aktas, C. Ceken, and Y. E. Erdemli, "IoT-based healthcare framework for biomedical applications," *J. Med. Biol. Eng. 2018*, vol. 38, no. 6, pp. 966–979, Dec. 2017. doi: 10.1007/s40846-017-0349-7.
[55] Y. Rbah *et al.*, "Machine learning and deep learning methods for intrusion detection systems in IoMT: A survey," in *2nd Int. Conf. IRASET*, Meknes, Morocco, 2022.
[56] E. Luo, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu and M. Atiquzzaman, "PrivacyProtector: Privacy-protected patient data collection in IoT-based healthcare systems," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 163–168, Feb. 2018. doi: 10.1109/MCOM.2018.1700364.

[57] N. Hajiheydari, M. S. Delgosha, and H. Olya, "Scepticism and resistance to IoMT in healthcare: Application of behavioural reasoning theory with configurational perspective," *Technol. Forecast. Soc. Change*, vol. 169, no. 4, pp. 120807, Aug. 2021. doi: 10.1016/j.techfore.2021.120807.
[58] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar and A. Farouk, "Secure medical data transmission model for IoT-based healthcare systems," *IEEE Access*, vol. 6, pp. 20596–20608, Mar. 2018. doi: 10.1109/ACCESS.2018.2817615.
[59] J. P. A. Yaacoub *et al.*, "Securing internet of medical things systems: Limitations, issues and recommendations," *Fut. Gener. Comput. Syst.*, vol. 105, no. 10, pp. 581–606, 2020. doi: 10.1016/j.future.2019.12.028.
[60] A. Chacko and T. Hayajneh, "Security and privacy issues with IoT in healthcare," *EAI Endorsed Trans. Pervasive Health Technol.*, pp. 155079, Jul. 2018. doi: 10.4108/eai.13-7-2018.155079.
[61] A. S. Adarsha, K. Reader, and S. Erban, "User experience, IoMT, and healthcare," *AIS Transact. Human-Comput. Interact.*, vol. 11, no. 4, pp. 264–273, 2019. doi: 10.17705/1thci.00125.
[62] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos and C. Douligeris, "Security in IoMT communications: A survey," *Sensors*, pp. 1–49, Aug. 2020. doi: 10.3390/s20174828.
[63] V. Subramaniyaswamy *et al.*, "RETRACTED ARTICLE: An ontology-driven personalized food recommendation in IoT-based healthcare system," *J. Supercomput.*, vol. 5, no. 6, pp. 3184–3216, Jun. 2019. doi: 10.1007/s11227-018-2331-8.
[64] M. Moqbel, M. S. Rahman, S. Cho, and B. Hewitt, "Sustaining patient engagement: The role of health emotion and personality traits in patient portal continuous use decision," *AIS Transact. Human-Comput. Interact.*, vol. 12, no. 4, pp. 179–205, 2020. doi: 10.17705/1thci.00135.
[65] L. Zhang, Y. Wu, L. Chen, L. Fan, and A. Nallanathan, "Scoring aided federated learning on long-tailed data for wireless IoMT based healthcare system," *IEEE J. Biomed. Health Inform.*, vol. 28, no. 6, pp. 3341–3348, 2023. doi: 10.1109/JBHI.2023.3300173.
[66] S. Hamadneh, I. Akourm, B. Al Kurdi, H. M. Alzoubi, M. T. Alshurideh and A. Q. M. AlHamad, "An IoMT-based healthcare model to monitor elderly people using transfer learning," in *Cyber Security Impact on Digitalization and Business Intelligence: Big Cyber Security for Information Management: Opportunities and Challenges*. Cham: Springer International Publishing, 2024, pp. 267–279.
[67] T. Abbas *et al.*, "Secure IoMT for disease prediction empowered with transfer learning in healthcare 5.0, the concept and case study," *2023 IEEE Access*, vol. 11, pp. 39418–39430, 2023. doi: 10.1109/ACCESS.2023.3266156.
[68] S. Abbas *et al.*, "Fused weighted federated deep extreme machine learning based on intelligent lung cancer disease prediction model for Healthcare 5.0.," *2023 Int. J. Intell. Syst.*, vol. 2023, no. 2, pp. 1–14, 2023. doi: 10.1155/2023/2599161.
[69] L. C. Fourati and S. Ayed, "Federated learning toward data preprocessing: COVID-19 context," in *Proc. ICC Workshops*, Montreal, QC, Canada, 2021.
[70] D. Gupta, O. Kayode, S. Bhatt, M. Gupta, and A. S. Tosun, "Hierarchical federated learning based anomaly detection using digital twins for smart healthcare," in *Proc. CIC*, Atlanta, GA, USA, Dec. 13–15, 2021, pp. 16–25.
[71] L. Rachakonda, S. P. Mohanty, and E. Kougianos, "iFeliz: An approach to control stress in the midst of the global pandemic and beyond for smart cities using the IoMT," in *Proc. ISC2*, Piscataway, NJ, USA, 2020.
[72] X. Hu, E. C. H. Ngai, G. Castellano, B. Hu, J. J. P. C. Rodrigues and J. Song, "Special issue on toward intelligent internet of medical things and its COVID-19 applications and beyond," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15649–15651, Nov. 2021. doi: 10.1109/JIOT.2021.3114575.
[73] A. Chauhan, K. Farmah, A. Goel, and A. Gandotra, "A novel patient monitoring system using photoplethysmography and IoT in the age of COVID-19," in *125th Int. Conf. (ICCMC)*, Erode, India, Apr. 08–10, 2021, pp. 427–437.
[74] I. Masood, W. Yongli, D. Ali, A. Naif Radi, and D. Hassan, "Towards smart healthcare: Patient data privacy and security in sensor-cloud infrastructure," *Wirel. Commun. Mob. Comput.*, vol. 2018, no. 2, pp. 1–23, 2018. doi: 10.1155/2018/2143897.

[75] F. Ali, H. Kumar, S. Patil, A. Ahmed, A. Banjar and A. Daud, "DBP-DeepCNN: Prediction of DNA-binding proteins using wavelet-based denoising and deep learning," *Chem. Intell. Lab. Syst.*, vol. 229, pp. 104639, Oct. 2022. doi: 10.1016/j.chemolab.2022.104639.

[76] F. Ali, H. Kumar, S. Patil, A. Ahmad, A. Babour and A. Daud, "Deep-GHBP: Improving prediction of growth hormone-binding proteins using deep learning model," *Biomed. Signal Process. Control*, vol. 78, no. 8, pp. 103856, Sep. 2022. doi: 10.1016/j.bspc.2022.103856.

[77] I. Masood, A. Daud, Y. Wang, A. Banjar, and R. Alharbey, "A blockchain-based system for patient data privacy and security," *Multimed. Tools Appl.*, vol. 83, no. 21, pp. 60443–60467, 2024. doi: 10.1007/s11042-023-17941-y.