IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 3 January 2024, accepted 26 January 2024, date of publication 5 February 2024, date of current version 12 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3362239

SURVEY

Empowering Healthcare With IoMT: Evolution, Machine Learning Integration, Security, and Interoperability Challenges

G. R. PRADYUMNA[1], **ROOPA B. HEGDE**[1], **K. B. BOMMEGOWDA**[1], **TONY JAN**[2], **AND GANESH R. NAIK**[2,3,4]

[1]NITTE (Deemed to be University), Department of Electronics and Communication Engineering, N.M.A.M. Institute of Technology, Udupi, Karnataka 574110, India
[2]Centre for Artificial Intelligence Research and Optimization (AIRO), Design and Creative Technology Vertical, Torrens University, Ultimo, NSW 2007, Australia
[3]Design and Creative Technology Vertical, Torrens University, Adelaide, SA 5000, Australia
[4]College of Medicine and Public Health, Flinders University, Adelaide, SA 5042, Australia

Corresponding author: Roopa B. Hegde (roopabhegde@nitte.edu.in)

This work was supported by NITTE (Deemed to be University).

ABSTRACT The Internet of Medical Things (IoMT) is the subset of the Internet of Things (IoT) that connects multiple medical devices, collect information/data from devices, and transmits and process data in real-time. IoMT is crucial for increasing electronic device accuracy, reliability, and productivity in the healthcare industry. IoMT has emerged as a next-generation bio-analytical tool that converges network-linked biomedical devices with relevant software applications for advancing human health. Adapting IoMT and associated technologies has fixed several problems using telemedicine, remote monitoring, sensors, robotics, etc. However, adopting IoMT technologies for a large population is challenging due to extensive data management, privacy, security, upgradation, scalability, etc. Although significant research has been carried out in this domain, identifying emerging trends and highlighting the technological advancement and challenges within IoMT is required for its success. Moreover, it will aid policymakers, scientists, healthcare practitioners, and researchers to measure the pertinence of IoMT in healthcare sectors more efficiently. This review discusses the evolution of IoMT, Machine Learning Integration, Security, and interoperability challenges of IoMT devices.

INDEX TERMS Internet of Medical Things, Internet of Things.

I. INTRODUCTION

The Internet of Medical Things (IoMT) is a revolutionary technology that connects multiple medical devices, collects information/data from the devices, and transmits and processes the data in real-time. This merges the healthcare workflow and the power of the Internet of Things (IoT) to create an ecosystem that enhances the workflow. A typical conceptual IoMT-based framework is shown in FIGURE 1. The figure shows IoMT, which can handle data from various devices ranging from simple sensors to sophisticated devices. The collected medical data consists of patient details; hence, data security is crucial in IoMT. Furthermore, the data are processed and analyzed in real-time, enabling continuous monitoring. Therefore, IoMT plays a prominent role in the healthcare industry.

Integrating medical devices, data collection, and connectivity offers healthcare systems a wide range of benefits. It enables remote patient monitoring, allows personalized treatment plans and care, allows large amounts of data collection, improves decision-making, and facilitates telemedicine and remote consultation. Thus, IoMT leverages the power of connected devices and data-driven technologies to revolutionize patient care and healthcare management. By enabling the real-time monitoring of patients' vital signs, chronic conditions, and medication adherence, IoMT empowers

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

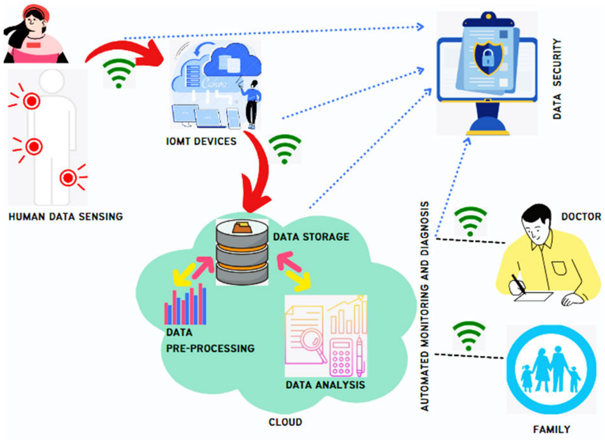

FIGURE 1. A typical IoMT-based smart healthcare system.

healthcare providers with timely and accurate insights. This leads to quicker diagnoses and more effective treatment plans, reducing hospital readmission.

Moreover, IoMT facilitates remote patient monitoring and extends care beyond hospitals. With the potential to enhance preventive care, IoMT can help identify health risks early and encourage proactive intervention. Additionally, the large amount and variety of data generated by IoMT devices can improve medical research, leading to innovations.

IoMT applications cover many healthcare domains, including telehealth, remote patient monitoring, hospital management, elderly care, patient medication management, and emergency care. Alshehri and Muhammad [1] highlighted aspects such as the IoT, IoMT, edge computing, cloud computing, medical signal fusion, security and AI by covering journal articles published between 2014 and 2020. As technology advances, IoMT promises healthcare innovation, improves patient outcomes, and makes healthcare more accessible and efficient for individuals and providers. IoMT benefits various entities, including patients, hospitals, doctors, and health insurance companies. Patients benefit from personalized care and directly connect with doctors via cloud storage. For instance, elderly patients with chronic vital signs (heartbeats, blood pressure, oxygen saturation, etc.) can be monitored using wearables. Doctors can access data from home-monitoring devices and wearables (cloud-connected), including patient history, and recommend medications or further treatment. This vital information helps with patient health tracking, access to diagnostic reports, and informed decision-making. Simultaneously, hospitals can track patients' data in real-time via embedded IoT devices connected to patients' homes, which helps diagnose infectious diseases. This is achieved via imaging devices (X-ray, MRI, CT scan, etc) and efficient management of inventory and monitoring devices, thus reducing costs. In addition, the IoMT framework helps manage the hospital protocols. Health insurance companies can significantly benefit from using Artificial Intelligence (AI) technology to capture patient case histories and store medical documents for investigation and fraud detection. It also helps promote transparency among patients, hospitals, and customers.

Similar to IoT, IoMT devices consist of perception and architecture layers. The perception layer signifies a variety of numerous smart medical devices collecting health data, and the connectivity layer is accountable for data transmission (perception layer to the cloud and vice versa). The processing layer stores and manages data using connectivity, gateway technologies, and with the help of cloud middleware or IoT platforms. Similarly, using software, the application layer provides end users with opportunities for device control, data analytics, and reporting.

Motivation

The IoMT is a rapidly evolving field with significant research and innovation. Reviewing articles in such a field allows us to integrate and consolidate existing knowledge, making it easier for researchers to obtain an overview of state of the art. Identifying emerging trends and highlighting the technological advancements and challenges within IoMT can be helpful for researchers planning future work. Many review articles addressing the issues and challenges in the IoMT framework can be found in the literature. However, most of these reviews only cover security, network concepts, and software designs. Moreover, the recent development of more complex and heterogeneous low-cost IoMT devices are resulted in numerous security and privacy issues. Hence, the primary motivation of this review is to provide in depth overview of recent advances in IoMT and an informative resource that summarizes various aspects of IoMT, such as the role of ML, data security and privacy issues, major challenges, and future directions. This would help researchers to identify the current requirements that lead to innovation.

II. IoT TO IoMT EVOLUTION

The evolution from IoT to IoMT represents a specialized branch that focuses on the integration of smart devices, sensors, and medical technology to revolutionize healthcare sector. Recognizing the unique requirements and opportunities within the healthcare sector drives the evolution of the IoT to IoMT. IoMT focuses on leveraging IoT technologies and principles to enhance healthcare delivery, improve patient outcomes, and provide patient-centric care while addressing the healthcare industry's specific challenges and regulatory considerations.

The transition from the IoT to the IoMT is not just a semantic shift. Still, it represents a significant adaptation of technology to meet the specific needs of healthcare, as shown in FIGURES 2 and 3.

The increasing demand for mobile, multisensor, and intelligent healthcare solutions has fueled this adaptation.

Furthermore, the design of IoMT devices mandates specific attributes, such as cost efficiency, low computational overhead, energy conservation, and wireless networking capabilities, to make them both practical and effective [2]. The core aim is to enhance healthcare delivery, improve

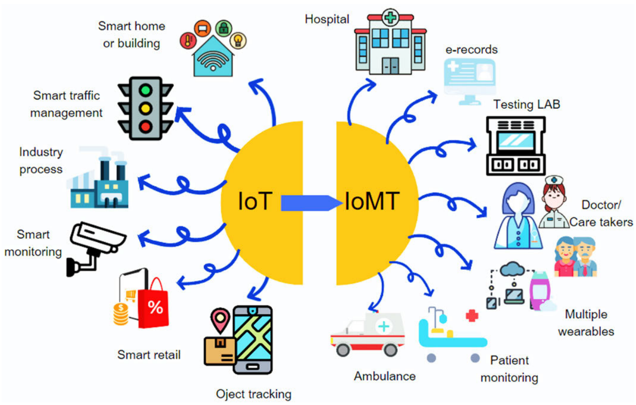

FIGURE 2. IoT to IoMT evolution.

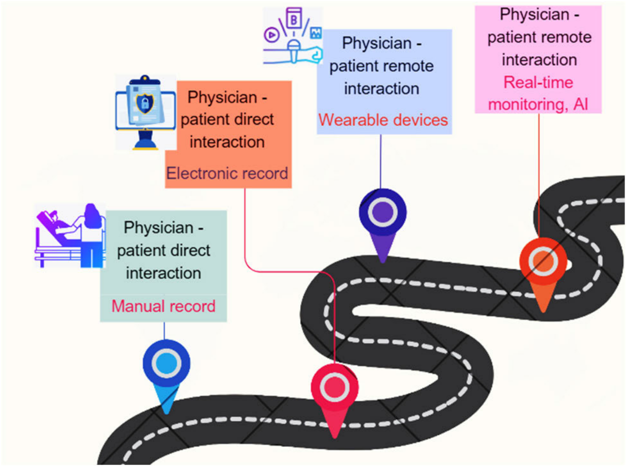
Physician - patient remote interaction
Real-time monitoring, AI
Physician - patient remote interaction
Wearable devices
Physician - patient direct interaction
Electronic record
Physician - patient direct interaction
Manual record

FIGURE 3. The transition from manual to digital and to cloud.

patient outcomes, and provide patient-centric care while navigating the complex landscape of regulatory considerations and industry-specific requirements [3]. This technological transformation has enabled ubiquitous access to medical services. IoMT encompasses medical devices, wearables, software, and systems that gather and transmit patient health data in real-time as shown in FIGURE 2. These devices include wearable fitness trackers, remote monitoring systems, smart implants, and more. However, there is a slow transition of the system from manual workflow to automated workflow as indicated in FIGURE 3. Challenge is to match automated workflow to that of manual.

The capabilities of IoMT extend beyond mere device interconnectivity; they pave the way for democratized access to healthcare. This accessibility can significantly enhance patient care and remote monitoring and improve health outcomes [3], [4]. In this evolving landscape, wearables are a vital subcategory within the IoMT ecosystem. They facilitate real-time data transfer between healthcare providers and patients. This is crucial in time-sensitive conditions, such as medical emergencies and disaster responses, and provides continuous health monitoring data valuable for preventive care and long-term treatment plans [5]. However, the interconnected architecture of IoMT presents a range of security challenges, including risks to data integrity and patient safety. Regulatory bodies and healthcare providers often find themselves in gray areas concerning compliance standards and security protocols expected from IoMT device manufacturers [6]. Researchers are developing novel security algorithms and protocols to safeguard IoMT edge networks and ensure data confidentiality and integrity [7].

Blockchain technology has emerged as a promising avenue for enhancing IoMT security. Its decentralized architecture provides robust mechanisms for data integrity and accountability while eliminating single points of failure. Given the resource-constrained nature of IoMT devices, lightweight blockchain architectures are being developed to balance security needs with storage and computational efficiencies [3], [8], [9].

Beyond the technical aspects, societal acceptance and long-term sustainability are key factors influencing the IoMT landscape. Sociotechnical studies have shown that the interplay between the social and technological dimensions is intricate and co-evolutionary. This understanding is critical when considering the broader implications of deploying next-generation IoMT networks [10].

The transition from IoT to IoMT represents a transformative shift with unprecedented opportunities and formidable challenges. Practical solutions, such as blockchain technology, can mitigate many security risks, while a nuanced understanding of the sociotechnical landscape can guide the successful deployment and acceptance of IoMT [11].

III. DATA HANDLING AND MACHINE LEARNING INTEGRATION IN IoMT

Integrating ML into IoMT for data handling has significantly advanced healthcare technology. IoMT devices generate enormous amounts of patient data, from vital signs to medication adherence records, stored as electronic health records (EHR). ML algorithms can analyze, interpret, and extract valuable insights from IoMT data, aiding in early disease detection, suitable treatment plans, and predictive healthcare. Thus, ML models enable healthcare providers to address individual patient needs. Moreover, integrating ML into IoMT enhances decision support systems, streamlines diagnosis, and continuously improves health care protocols. However, this integration also places significant importance on data security and privacy as sensitive medical information becomes the basis for informed medical decisions and personalized care plans. Integrating data handling and ML within the IoMT can revolutionize the healthcare system by enabling accurate, timely, and patient-centric medical interventions.

This section highlights the role of different ML algorithms in various aspects of IoMT systems. ML algorithms can be broadly classified into supervised, unsupervised, and reinforcement learning techniques, as shown in FIGURE 4. Each type has a role in IoMT that revolutionizes healthcare by enabling advanced data analysis and decision-making

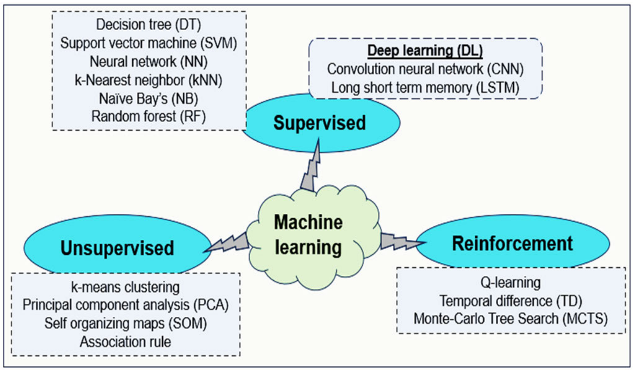

FIGURE 4. **Types of ML algorithms and commonly used algorithms under each type.**

processes. Supervised learning involves training algorithms on labeled data to make accurate predictions or classifications. These algorithms can aid in diagnosing medical conditions, monitoring patient health, and predicting disease progression. However, these algorithms require a large amount of training data. Unsupervised learning techniques can be employed in IoMT to uncover hidden patterns and structures within the unlabeled data. These methods enable clustering, anomaly detection, and data exploration, providing insights into patient trends, population health, and potential outbreaks. Reinforcement learning within IoMT pertains to training algorithms to make sequences of decisions based on trial and error and optimize actions over time.

This approach finds applications in personalized treatment plans, adaptive therapies, and optimizing medical interventions. Hence, incorporating these ML techniques into IoMT promises to improve patient outcomes, enhance medical research, and drive innovation in healthcare.

A. SIMULATION-BASED MONITORING AND PREDICTIVE ANALYSIS IN IoMT

In the healthcare sector, IoMT constitutes a network of interconnected medical devices and software designed to gather, process, and analyze medical information. AI and ML play a vital role by enabling advanced data analysis, automated prediction, and improved decision-making capabilities, which can significantly improve the speed and accuracy of diagnosis [12]. ML algorithms can process and analyze vast amounts of medical data generated from IoMT devices such as wearable sensors, remote monitoring tools, and medical imaging equipment. They can quickly identify patterns, trends, and anomalies in the data fed to them, enabling healthcare professionals to gain deeper insight into patient conditions, disease progression, and treatment efficacy. On the other hand, ML models can be trained to predict health conditions based on historical data, allowing healthcare providers to make early diagnoses and personalized care [13]. This enables timely interventions and reduces the need for frequent in-person visits to healthcare facilities, thereby allowing remote patient monitoring. These aspects were emphasized in a comprehensive study by Manickam et al. [14]. ML algorithms can also provide personalized recommendations that help improve treatment outcomes and reduce adverse effects. Hence, ML has revolutionized medical imaging and signaling analysis, enabling the automated detection and diagnosis of diseases. ML algorithms can accurately identify patterns that may be challenging for human experts to detect, leading to faster and more accurate diagnosis.

Compared with other predictive and diagnostic analysis types, extensive applications of supervised ML algorithms are commonly found in the literature. An experimental study by Nigar et al. [15] employed multiple supervised ML models to detect and monitor chronic diseases using IoMT data and obtained promising results. DL architectures, namely ResNet 18 and googleNet, were employed by Dahan et al. [16] for predicting abnormal data. Yildirim, et al. [17] analyzed IoMT-based verbal data for the COVID-19 early diagnosis by employing RF and Gradient Boosted Tree (GBT) in real-time scenarios and obtained an accuracy of approximately 95%. Thandapani et al. [18] attempted to classify X-ray/CT images to rank the severity of COVID-19 whenever a person uploaded the images. To accomplish this, experiments utilizing various deep CNN architectures, including ResNet-50, ResNet-100, ResNet-101, VGG-16, and VGG-19, were conducted, and the highest accuracy of 97% was achieved through the ResNet-101 architecture. A novel idea proposed by Jaba Deva Krupa et al. [19] demonstrated the potential of DL in the non-invasive remote monitoring of fetal health. The study detected the fetal QRS complex without removing maternal signals in the abdominal ECG. Using sensor data and ML algorithms, Dutta et al. [20] processed IoMT traffic and predicted a patient's health condition. This study demonstrated that ML can transform raw IoMT traffic data into understandable patterns, enabling better decision-making. A survey by Bibi et al. [21] provided an IoMT-based framework for leukemia detection by linking cloud computing and clinical gadgets. A simulation-based method employing deep belief networks with a CNN (DBN-CNN) predicted diabetes in patients with cardiac issues. Sampathkumar et al. [22] provided promising results when the gravitational search optimization (GSO) algorithm was adapted in the data pre-processing step. The effectiveness of supervised ML algorithms, such as SVM, k-NN, and DT, was analyzed by Khan et al. [23] for monitoring older adults. This study utilized IoMT datasets to evaluate the performance of the algorithms. Recently, Jarrah et al. [24] investigated the usability of DL algorithms for monitoring older adults using IoMT data and achieved an average accuracy of approximately 93%. An extensive study by Al-Hajjar and Al-Qurabat [25] elaborated on how ML algorithms can enhance seizure detection using an IoMT-based EEG signal analysis. The current lifestyle affects stress levels, requiring early detection and continuous monitoring to maintain mental health. Rachakonda, et al. [26] proposed a smart mirror to detect stress in an IoMT framework, obtaining an accuracy of approximately 97%. The same research group also proposed an intelligent device for monitoring food intake and stress levels and achieved an accuracy of approximately 98% using this approach. Proper food intake and diet are essential for maintaining good health. It also plays a significant role in the speedy recovery of patients on medication. Usually, nutritionists suggest diet plans based on patient health records. Iwendi et al. [27] automated this workflow, developed an assisted diet recommendation system, and obtained the highest accuracy (approximately 97%) using the DL approach.

Accurate ground truth or data labels are essential for supervised ML algorithms. However, obtaining these labels for medical data is challenging. Consequently, the adoption of unsupervised learning methods has become popular. Elbasi and Zreikat [28] compared the performances of both supervised and unsupervised ML algorithms to predict heart diseases using IoMT data and yielded comparable results regarding their outcomes. This suggests unsupervised ML methods can be adopted in IoMT systems without labelled data. IoMT architectures involve integrating multiple edge devices; hence, data in various formats are continuously sent to the cloud or storage devices for further processing. This can lead to data traffic, making data management and analysis challenging. The utilization of unsupervised ML algorithms, such as fuzzy c-means, to manage data traffic can be found in the literature [29]. This method demonstrated clustering techniques for numerosity reduction, which can facilitate a fast analysis. IoMT-based emerging healthcare offers many services, including cyborgs, a combination of AI robots, and doctors performing surgeries remotely. Tiwari et al. [30] introduced a federated reinforcement learning policy for robot-based knee replacement procedures, reducing the processing time by 50% compared to the conventional ML approach.

Understanding the dynamic interaction between these technologies is essential to explain the monitoring capabilities facilitated by deep learning within the IoMT framework. IoMT devices, such as wearable sensors and remote monitoring tools, continuously collect health-related data like vital signs, imaging data, and other physiological parameters. This data is then fed into DL algorithms, trained on extensive datasets to recognize patterns, anomalies, and trends indicative of health status changes. For instance, DL algorithms can analyze data from wearable electrocardiogram (ECG) sensors in cardiac health monitoring to detect arrhythmic events or other cardiac anomalies [19]. A specific case study worth noting involves the application of convolutional neural networks (CNNs) for real-time analysis of ECG data to predict potential cardiac events. This approach allows for timely interventions, reducing the need for frequent hospital visits and enabling proactive management of cardiac conditions. By continuously learning from new data, these DL models adapt and improve their predictive accuracy, thereby enhancing the efficacy of health monitoring in the IoMT ecosystem. This dynamic, data-driven approach exemplifies how DL transforms raw IoMT data into actionable insights, leading to improved patient outcomes and more efficient healthcare delivery.

B. REAL-TIME MONITORING AND PREDICTIVE ANALYTICS IN IoMT

Most of the studies mentioned above were conducted using stored data. However, in IoMT, the uninterrupted connectivity of medical devices to the network enables real-time monitoring of patients. Thus, the system involves seamless data acquisition, transmission, and analysis. In such applications, the major challenges are data privacy, data security, and obtaining quick responses from automated systems. These aspects were highlighted in a comprehensive study by Wagan et al. [31].

Along with physical well-being, mental health is essential for an individual's overall health and wellness. Many researchers have addressed this issue by proposing real-time systems using IoMT data, which can be found in a study by Gupta et al. [32]. This review highlighted the overview and challenges in real-time mental health analysis on two primary datasets: IoMT and social media. Raj et al. [33] explored real-time medical data analysis by introducing edge computing to reduce the burden on the cloud servers. In addition, the authors discussed the challenges of edge computing. In recent years, a real-time IoMT framework has been developed for the early detection of COVID-19 [17] and for monitoring elderly patients [34]. Social distancing was a crucial measure to prevent the rapid spread of Covid-19. Technologies played a vital role in this period, particularly in the remote monitoring of patients, and Aljabr and Kumar [35] introduced one such technology. Nowadays, patient monitoring is not limited to physical parameters but is extended to monitor brain activities to provide timely treatment, especially for stroke-related cases. This is evident from the proposal of a wearable device by [36] to enable remote monitoring and analysis of brain signals in real-time scenarios.

The complexity of ML algorithms increases in real-time applications. This is because, in the IoMT framework, medical devices and sensors are integrated into the network, generating various types of vast amounts of data. Extracting useful information and insights from data is crucial for making predictions and deciding on further necessary actions in real-time scenarios. This involves several steps: data pre-processing, handling imbalanced data, predictive and diagnostic analysis, and real-time analysis, enabling continuous monitoring. In addition, it is necessary to address the energy efficiency of IoMT devices, resource availability, and network scalability.

1) DATA PRE-PROCESSING AND FEATURE ENGINEERING FOR IoMT DATA

In healthcare, data come in diverse formats: text, speech or audio, signal or time series, and images from different modalities. Each provides unique insights into patients' health and medical conditions. Hence, efficient data handling and

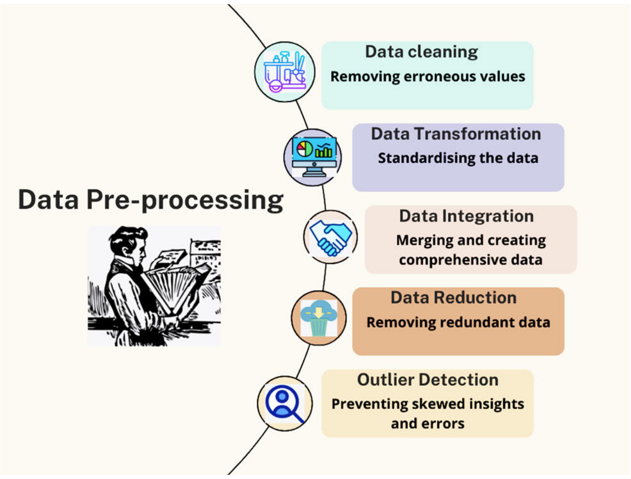

FIGURE 5. Data pre-processing steps.

processing techniques are required to unlock the complexities of healthcare data. In ML, these are referred to as data pre-processing and feature engineering. Data pre-processing involves several steps, as shown in FIGURE 5. Implementing these steps improves the effectiveness of ML algorithms when training them with pre-processed data. In IoMT, medical devices communicate and share sensitive data through the network; hence, detecting intruders in the architecture that the attackers would otherwise change is crucial. Therefore, data pre-processing in the present article includes identifying intruders. However, it is not included in FIGURE 5 because this step applies to handling IoMT data and does not apply to the general pipeline.

Nickolas and Shobha [37] experimentally demonstrated the importance of data pre-processing for achieving high performance using ML algorithms. Details of several pre-processing techniques can be found in a review article by Fan et al. [38].

IoMT devices generate vast volumes of data from various sensors, wearables, and medical instruments, making it imperative to identify and prioritize the most relevant features for analysis. By selecting the correct set of features, the computational complexity can be reduced, model performance can be improved, and quicker decision-making can be facilitated. A study by Islam et al. [39] highlighted five feature selection methods suitable for IoMT analysis, which include: i) Random Forest, ii) Normalized Mutual Information Feature Selection (NMIFS), iii) Minimum Redundancy - Maximum Relevance (mRMR), iv) F-Test, and v) Chi-Square test.

Healthcare data are sensitive, and it is necessary to develop an automated system to avoid potential risks associated with unauthorized access or tampering with sensitive data. Thus, tampering may affect the diagnostic results. Hence, it becomes crucial to detect intrusion before data analysis and after analysis at the receiving end. Several intrusion detection studies have been proposed based on the ML approach in recent years. Many supervised and unsupervised ML algorithms have been proposed for identifying and classifying anomalies. A review article by Hernandez-Jaimes et al. [40] provided a taxonomy of intrusion detection systems, discussing AI-based methods and legal and ethical security aspects. Rbah et al. [41] compared and analyzed the performances of different ML and DL methods for detecting and preventing network attacks, emphasizing the performance and limitations of these methods. Experimental evidence confirmed that data pre-processing steps, especially data cleaning and reduction, were essential for intrusion detection [42]. An intrusion detection system using the DL approach [43], [44] and DL and ML approaches [45] adapted feature selection and data pre-processing to increase efficiency. These studies implied that data pre-processing was mandatory in the ML-based IoMT framework. A comparison of supervised ML algorithms, namely k_NN, NB, SVM, ANN, and DT, for intrusion detection using the Bot IoT dataset was performed by Binbusayyis et al. [46], providing a promising path to discover a suitable algorithm. The essential aspects of the clustering technique, an unsupervised ML algorithm, were highlighted by Guan et al. [47] and reinforcement learning by Guan et al. [48] for achieving data privacy in IoMT systems. The reinforcement learning approach improved the network performance even in the presence of traffic volume differences.

2) HANDLING IMBALANCED DATA TO IMPROVE IoMT MODEL PERFORMANCE

Imbalanced data are cases in which one class significantly outnumbers the other, which can lead to biased and inaccurate predictions. In IoMT, this can result in misdiagnosis or ineffective medical intervention. Several strategies have been employed to address this challenge and ensure reliable model outcomes, such as resampling, synthetic data generation, ensemble methods, and cost-sensitive learning. Hence, data analytics and understanding these insights are major tasks that need to be addressed in the IoMT system. Soleimani and Mirsha Zadeh [49] emphasized various methods for handling imbalanced data for multiclass problems. However, this was a general study using an imbalanced dataset. Toor et al. [50] addressed a specific application to manage imbalanced IoMT data. A feasibility study by Ha et al. [50] addressed data security and imbalance considering the COVID-19, X-ray, and cholesterol datasets.

Addressing imbalanced datasets in the IoMT framework is essential for identifying patterns from sensitive healthcare data. Employing techniques such as data resampling, algorithm selection, and evaluation metrics can help develop effective and reliable systems that can provide quick and accurate decisions.

3) ENSURING NETWORK SCALABILITY AND BANDWIDTH REQUIREMENTS

In healthcare, the demand for real-time data exchange and remote monitoring has rapidly increased, putting pressure on the network infrastructure. Scalability involves designing networks that can easily accommodate the growing number of IoMT devices and the data they generate. This scalability ensures that healthcare facilities can expand their IoMT ecosystems without suffering network congestion or performance degradation. Meeting bandwidth requirements is equally essential, as medical data, such as high-resolution images, video feeds, and patient records, can be data-intensive. Adequate bandwidth ensures quick data transmission, thus enabling timely diagnosis. To achieve scalability and higher bandwidth, IoMT frameworks employ advanced networking technologies, including edge computing, load balancing, QoS policies, and robust network architecture planning. By ensuring network scalability and meeting bandwidth demands, IoMT not only improves the efficiency of healthcare delivery but also paves the way for innovative medical applications that rely on seamless, high-speed data connectivity.

4) RESOURCE OPTIMIZATION AND ENERGY EFFICIENCY FOR IoMT DEVICES

Patient monitoring, diagnostics, and data collection in the healthcare sector rely on connected devices. Hence, managing resources and energy consumption effectively has several critical implications. First, optimizing resource usage ensures that IoMT devices function efficiently and provide uninterrupted healthcare services. This includes optimizing the memory, processing power, and communication bandwidth to meet the demands of real-time data processing and transmission. Second, energy efficiency is essential for extending the battery life of wearable devices, reducing the need for frequent recharging or battery replacement. Prolonged battery life enhances user convenience and reduces the maintenance burden for healthcare providers.

Moreover, for IoMT wearable devices, energy efficiency is vital because frequent discharge or battery replacement may pose risks and inconveniences. Intelligent power management, data compression, and energy-efficient communication protocols can be adapted to achieve these goals. IoMT devices can provide reliable, durable, and sustainable healthcare solutions by prioritizing resource optimization and energy efficiency and improving patient care quality.

ML algorithms can help optimize healthcare resource allocation, enabling healthcare organizations to allocate resources more efficiently and provide timely care. Real-time systems allow both patients and professionals to access and respond appropriately. However, this leads to inefficient network utilization. An unsupervised ML algorithm proposed by Sugadev et al. [51] balanced the network demand based on several nodes and predictive rates, thereby enhancing the network speed. An experimental investigation by Ali et al. [52] found that a feed-forward bidirectional LSTM algorithm improved the quality of service (QoS) in a 5G network for predicting heart diseases. An unsupervised ML-based software-defined network (SDN) architecture Haseeb et al. [53] indicated that network resource consumption would improve data delivery and decrease communication overhead. A crucial step in the real-time IoMT framework is establishing reliable communication among devices connected to the patient, the cloud computing environment, and healthcare professionals. Utilization of reinforcement learning by Nazari et al. [54] provided an optimal path between the nodes, increasing QoS and energy efficiency. Priya and Malhotra [55] employed a double-reinforcement learning technique to obtain an optimal network selection policy. The simulation results demonstrated an improvement in system utility. A summary of the data handling and processing in IoMT is presented in TABLE 1.

IV. SECURITY AND PRIVACY IN IoMT

The need for security and privacy in IoMT is vital due to the sensitive nature of healthcare data. Security measures are essential to protect against cyberattacks, unauthorized access, and data breaches that could interfere with patient privacy-ensuring data encryption, robust access controls, and device security safeguards against hostile individuals, taking advantage of weaknesses in IoMT systems. Furthermore, compliance with healthcare regulations is mandatory to uphold patient rights and maintain the trust of both patients and healthcare providers. Ethical considerations, such as obtaining informed consent and transparent data practices, are fundamental to respecting individual autonomy and preserving the integrity of health care data. In IoMT, security and privacy are not only regulatory requirements but also the foundations for safe and effective healthcare delivery. Sun, et al. [58] highlighted the importance of data security, patient security, access control, and cyber threats by reviewing the state-of-the-art methods. In addition, Alhaj et al. [59] justified the need to investigate and address security issues in the IoMT framework. The present review includes literature on four data security and privacy aspects, as shown in FIGURE 6.

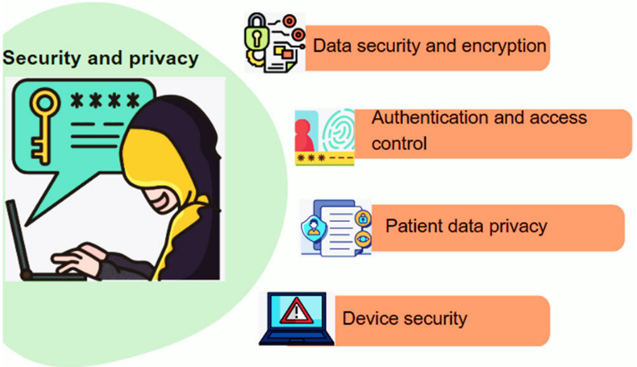
Security and privacy
Data security and encryption
Authentication and access control
Patient data privacy
Device security

FIGURE 6. Critical aspects of security and privacy in IoMT.

TABLE 1. Summary of data handling and processing in IoMT.

Authors	Conceptual framework	Real-time System	Approach and dataset	Metrics and results	Major findings
Nigar, et al. [15]	Early diagnosis and monitoring of six chronic disorders, including i) pneumonia, ii) diabetes, iii) heart disease, iv) brain tumor, v) Alzheimer's, and vi) COVID-19.	No	Supervised DL: DenseNet, VGG16, ResNet, VGG19, Inception-v3. COVID-19, diabetes, heart diseases (numerical, categorical data: 310,420,500) , brain tumor, pneumonia,Alzheimer's (images: 4262, 6360, 2000)	Precision, recall, accuracy, F1 score, AUC, ANOVA test. Accuracy: 80%	Statistical analyses showed significant differences with different classifiers. However, the ML approach helps doctors in the early detection and diagnosis of chronic health conditions.
Dahan, et al. [16]	AI-based, IoMT telemedicine framework for E-healthcare - monitoring body parameters, namely BP, heart rate, temperature, blood glucose level, SPo2.	No	Supervised DL: LDA, cuckoo search, hybrid ResNet18- GoogleNet. 50 patients between 50 and 70 years (numerical data)	Precision, recall, accuracy, F1 score, miss rate, execution time, and computation time. Accuracy: 99.69%.	The ML-based system helps supervise patients' vital parameters, detect anomalies, and provide timely alerts to care givers, improving patient outcomes, reducing hospital readmissions, and enhancing the overall quality of healthcare delivery.
Yildirim, et al. [17]	IoMT framework for early identification and diagnosis of COVID-19.	No	Supervised ML: RF, GBT Created a dataset using Riverbed Modeler simulation software and verbal data: a total of 278,848 records.	Precision, recall, accuracy, F1-Score, receiver operating characteristic (ROC) curve. Accuracy: 95.7%	The IoMT framework can quickly detect and send information on COVID-19-positive cases to healthcare institutions.
Thandapani, et al. [18]	A responsive system for delivering medical services to patients lacking adequate medical facilities.	Yes	Supervised DL: ResNet-50, ResNet-100, ResNet-101, VGG 16, VGG 19. X-ray images (2200), CT images (1700), text data.	Precision rate, recall rate, accuracy, F1-Score. Accuracy: 97%	CT images are more suitable than X-ray images to detect COVID-19. ResNet101 and VGG 19 outperformed.
Jaba Deva Krupa, et al. [19]	Remote monitoring of fetal health using abdominal ECG signals uploaded to the cloud.	Partial	Supervised DL: Hilbert Huang Transform (HHT), Stockwell transform (ST), MobileNet, ResNet18. 2013 challenge database.	Accuracy, precision, recall, F1-Score. Accuracy: 88.7%	ST, in combination with Mobilenet improves the analysis performance. However, there is a need for a stand-alone device for real-time scenarios.
Dutta, et al. [20]	Monitoring and prediction of health status. Monitoring IoMT traffic.	No	IoT-Flock traffic generator, WEKA, Supervised ML: NB, LR, Unsupervised ML: k-NN, k-means. Dataset - NA	MSE, MAE, RMSE, accuracy.	Conventional ML techniques help in monitoring both health status and IoMT traffic.

TABLE 1. ***(Continued.)*** **Summary of data handling and processing in IoMT.**

Sampathkumar, et al. [22]	Cardiac risk prediction analysing diabetes data.	No	Supervised DL: GSOA, DBN-CNN, Supervised ML: SVM. Dataset: 100,000 records comprising 55 attributes.	Accuracy, precision, recall, F1-score, PSNR. Accuracy: 98%	Data optimisation helps to improve the model performance. However, there is a need for hybrid ML techniques to improve efficiency.
Khan, et al. [23]	Monitoring older adults accessing wearable device data.	No	Supervised ML: SVM, DT, ANN, Unsupervised ML: k-NN Dataset: 4848 records	Precision, recall, fscore, accuracy, ROC, miss rate Accuracy: 91.8%	The conventional ML approach could be used for monitoring older adults. However, a fusion-based ML approach may improve the performance.
Jarrah, et al. [24]	Assisting and monitoring older adults.	No	Supervised DL: DELM Dataset: 929 samples	Accuracy, sensitivity, specificity, miss-rate. Accuracy: 98.18%	ML techniques in IoMT framework reduce the response time, especially in emergencies.
Rachakonda, et al. [26]	Stress monitoring by developing iMirror: a device for maintaining healthy stress responses among individuals.	Yes	Image processing and supervised ML models. Dataset: 1000 images.	Precision, Recall, Accurate Precision (AP), Confidence. Accuracy: 97%	Mobile application-based systems help in assessing stress levels. However, adding potential remedies based on stress levels may help in healing.
Rachakonda, et al. [56]	Monitoring food intake and stress level by developing iLog: a wearable device (glass) for remote monitoring.	Yes	Image processing, Unsupervised DL: RCNN. Dataset: 1000 images.	Precision, Recall, AP, Confidence. Accuracy: 98%	Developed iLog has In-Cloud, In-Edge and In-Sensor based computational capability. However, lightweight ML models may reduce computational complexity and time.
Iwendi, et al. [27]	Automated system for detecting patients' food intake depending on disease and other features like demography and nutrient factors.	No	Supervised ML: LR, NB, RNN, MLP, GRU, LSTM. Dataset: 30 patients' data with 13 features - different diseases and 1000 products.	Accuracy, recall rate, precision rate, F1-measures. Accuracy: 97.74%	LSTM provides better results compared to the other models.
Elbasi and Zreikat [28]	Prediction of chronic illness	No	Supervised ML: RF, Hoeffding Tree, EM, NN, SVM, DT, Unsupervised ML: k-means, density, filtered, farthest clustering. Dataset: collected from wearables, ambulance, medical imaging, patient history, doctor reports, and labs.	Accuracy, precision, MCC, PRC, MAE, RMSE. Accuracy: 93%	Both supervised and unsupervised ML algorithms can be used to predict chronic diseases. However, information fusion and IoT algorithms may help improve the model's performance.
Kumar, et al. [29]	Segregation of biomarker data and generation of summarized data for each subject.	No	Unsupervised ML: Fuzzy c-means clustering, Supervised ML: CNN Publicly available WESAD dataset	Accuracy, F1-score, execution time. Accuracy: 72% - 96%	Using data clustering techniques aids real-time data streams in intelligent data analytics and enables quicker analysis.

TABLE 1. ***(Continued.)*** **Summary of data handling and processing in IoMT.**

Tiwari, et al. [30]	Cyborg for knee replacement procedure	Yes	RL: federated reinforcement learning, socket remote procedure call Dataset NA	-	
Debauche, et al. [34]	RAMi: a Real-Time Architecture for the monitoring of elderly patients	Yes	ML algorithms, Arduino, and ESP8266. ECG data	Measured body parameters were in line with the expected values	Adaptive architecture as needs or particularities changes make the architecture hopefully more sustainable. However, handling time series data is a challenge.
Binbusayyis, et al. [46]	Detection of intrusion in IoMT framework.	No	Unsupervised ML: k-NN, Supervised ML: NB, SVM, ANN, DT. benchmark dataset Bot-IoT	Accuracy, precision, recall, F1-Score, False alarm rate. Accuracy: 94% - 100%.	ML approaches effectively detect intrusion and can safeguard IoMT networks against malicious activities. However, efficiency needs to be improved in cases of imbalanced datasets.
Guan, et al. [47]	Private data clustering methods for IoMT.	No	Unsupervised ML: Clustering algorithm. Two datasets, Blood and Adult, from the UCI Knowledge Discovery Archive database.	MSE, Accuracy, response time	Optimized privacy budget sharing and initial centroids selection to improve the private K-means clustering algorithms's accuracy.
Guan, et al. [48]	Two-tier scheduling algorithm to improve channel utility and network throughput and decrease the delay.	No	RL: DRL	-	RL provides a data transmission guarantee for the communication network during large data analysis and guarantees the network performance, ensuring timely data transmission and improving the network quality.
Toor, et al. [57]	Enhanced Reactive Drift Detection Method methodically creates strategies to handle concept drift with a class imbalance in data sets.	No	Supervised ML, Recursive and enhanced recursive algorithm 48 synthetic datasets and real-world dataset	Accuracy, evaluation time, average prediction error Accuracy: 43% - 92%	Detection of drift types is needed. However, it is challenging to acquire such data streams. Moreover, it is a complex task to Generalize those algorithms. Addressed imbalance dataset.
Ha, et al. [50]	This method helps a secure medical data transfer between several hospitals	No	Supervised DL: CNN CT scans, X-rays, and cholesterol level medical data.	Accuracy, RMSE	In real-time scenarios, original patient data is encrypted to address patient privacy issues.
Sugadev, et al. [51]	Prediction of network resource consumption.	Yes	Software-enabled network (SDN).	Network throughput, % packet drop, response time Throughput: 95%	The approach enhances network speed as the number of nodes and data production rate varies. However, the overload link is not addressed by the authors.
Ali, et al. [52]	Prediction of heart disease with enhanced QoS	No	Supervised DL: Bi-directional LSTM. Dataset: The UCI Machine Learning Repository.	Accuracy, precision rate, recall rate. Accuracy: 97%	5G networks may be used for predictions of heart diseases, adopting widespread automation.
Haseeb, et al. [53]	Consumption of network resources and improved	No	Supervised ML model, SDN	Network throughput, packet	ML models improve the QoS. However, scalability needs to be

TABLE 1. *(Continued.)* **Summary of data handling and processing in IoMT.**

	sensor data delivery using ML with SDN-enabled security network.			drop ratio, data delay, and faulty packets. Network throughput increased by 21%	enhanced. DL approach can be explored.
Nazari, et al. [54]	Providing a reasonable level QoS for IoMT traffic.	No	RL	Average end-to-end delay, Total energy consumption, packet delivery ratio	Simulation results showed a reduction in energy consumption. However, implementation in real-time scenarios remains an open challenge.
Priya and Malhotra [55]	Optimal network selection policy. iMNet: RAT selection framework.	No	Double RL	Data Rate, delay, PLR, energy efficiency, cost.	Improvement in overall system utility. However, system convergence and complexity is a major challenge.

A. DATA SECURITY AND ENCRYPTION IN IoMT DEVICES AND NETWORKS

Encryption and data security are essential for guaranteeing the integrity and privacy of data in IoMT networks and devices. Medical devices collect and handle private health information, so strong security measures must be implemented to safeguard user privacy. However, miniaturized IoMT devices often have limited computational power, which poses challenges in implementing strong security schemes. Researchers have proposed various data security and encryption approaches in the IoMT to address these challenges.

Sun et al. [58] surveyed the state-of-the-art security and privacy approaches for IoMT-enabled healthcare systems. The survey highlighted the importance of encryption in protecting sensitive data in IoMT devices and networks. Masud et al. [60] proposed a lightweight and robust secure key establishment protocol for IoMT in COVID-19 patient care. Their research protocol utilized encryption techniques to ensure the confidentiality and integrity of the data exchanged between IoT nodes in medical networks. Another literature review by Hamza et al. [61] investigated IoT security and privacy risks and the limitations of IoT devices in applying data security and privacy algorithms. The study highlighted the challenges of confidentiality and integrity in IoT and discussed different schemes, such as the Key Management Scheme (KMS) and the Public Key Infrastructure algorithm, used to address these challenges.

Atamli and Martin [62] presented a threat-based security analysis for the IoT, discussing various technologies, security requirements, and the implications of centralized and distributed architectures on security aspects. The lack of holistic analysis and risk assessment in addressing security and privacy issues in IoT has also been highlighted. Data security and encryption in IoMT devices and networks are crucial for maintaining the privacy and integrity of sensitive medical data. Several studies have addressed security challenges and proposed solutions in this area. Li et al. [63] surveyed the security of blockchain systems, which are increasingly used in IoMT applications. The survey examined the security threats to blockchain and reviewed real blockchain security threats and actual attacks on popular blockchain systems.

Additionally, it covered ways to improve blockchain security and made recommendations for future research areas in this field. Sadeghi et al. [64] addressed the security and privacy challenges in industrial IoT systems, which are also relevant to IoMT. They highlighted the potential impact of cyberattacks on IoT systems and the need for a holistic security framework to address these challenges. This study provided an overview of the security and privacy challenges in the industrial IoT and discussed possible solutions.

B. AUTHENTICATION AND ACCESS CONTROL FOR IoMT SYSTEMS

Mechanisms for access control and authentication are essential to guaranteeing the security of IoMT systems. The increasing prevalence of IoMT devices has made it more challenging to manage and maintain the security of these systems. Adversaries can carry out cyberattacks by taking advantage of vulnerabilities in systems and networks. Therefore, robust mutual authentication and access control schemes are required to protect IoMT networks from adversarial threats. In this regard, Masud et al. [60] highlighted the absence of robust mutual authentication and key establishment schemes as key factors attracting adversaries to IoMT networks. Existing mutual authentication schemes are often computationally and communication-expensive, which can drain the energy reserves of IoT sensor nodes. To overcome these problems, the authors suggested a mutual authentication and secret key establishment technique for IoMT networks that is both lightweight and physically secure. The protocol utilised Physical Unclonable Functions (PUF) to verify the legitimacy of doctors and sensor nodes before establishing a session key. This approach ensured authentication, confidentiality, integrity, and anonymity in IoMT networks. Various methods before 2021 can be found in a review article by Hasan et al. [65], including security threats, data vulnerabilities, and countermeasures for 5G-enabled IoMT. This review has underlined the importance of encryption techniques, including access control, identity verification, and data encryption, in improving IoM device security and reliability. The lack of reliable authentication mechanisms and network access controls in IoMT devices has been identified as a major vulnerability. Gupta et al. [66] addressed privacy and security issues, such as confidentiality, entity authentication, and integrity using lattice-based data authentication and access control protocols that provide applicability in resource-constrained quantum environments.

C. ENSURING PATIENT PRIVACY IN IoMT ENVIRONMENTS

Ensuring patient privacy is a critical concern in IoMT. The sensitive nature of personal health data requires robust privacy-preservation mechanisms to protect patient information. Sun et al. [58] conducted a review that focused on the security and privacy requirements regarding data flow in different layers of IoMT systems. This study highlighted the importance of privacy preservation in e-healthcare environments.

Various approaches have been proposed to address privacy-preservation issues. Sahi et al. discussed privacy preservation issues in e-healthcare environments. They emphasized the need for privacy-preserving techniques to protect patient data in IoMT systems. In addition, they highlighted the importance of secure sessions in protecting virtual medical facilities from adversarial threats. Secure sessions ensure that sensitive information exchanged between IoT nodes over vulnerable wireless media remains protected [60].

D. CYBERSECURITY THREATS AND VULNERABILITIES IN IoMT

Cybersecurity threats and vulnerabilities pose significant risks to the IoMT systems. Interconnected medical devices in IoMT environments are susceptible to attacks and threats, as shown in FIGURE 7. Weak or default passwords lead to unauthorized access, allowing hackers to breach sensitive data and manipulate the devices. Additionally, inadequate data encryption and poor storage practices enable unauthorized users to use sensitive data and devices. The IoMT framework requires regular updates of software and security algorithms, which would otherwise lead to an attack of malware or ransomware that can disrupt device functionality, resulting in data loss. Sometimes, security is disrupted due to inadequate hospital staff training or misuse of facilities. Nowadays, Denial of Service (DoS) attacks are common because of the limited bandwidth or available processing power. Attackers use these limitations by overloading IoMT systems with traffic, disrupting their functionality, and potentially delaying patient care.

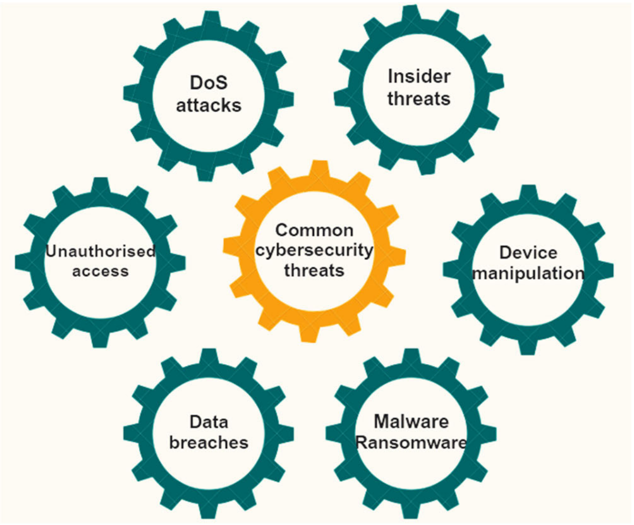

FIGURE 7. Common cybersecurity threats and vulnerabilities in IoMT.

Williams and McCauley [67] reviewed the vulnerabilities of interconnected medical devices in an IoMT environment. They highlighted the need for robust security measures to mitigate these vulnerabilities. Researchers have proposed comprehensive security frameworks for addressing cybersecurity threats and vulnerabilities. Sun, et al. [58] surveyed and reviewed security and privacy challenges, requirements, and threats in the IoMT domain. The survey provided insights into state-of-the-art approaches to addressing IoMT systems' cybersecurity threats. Alsubaei et al. [6] published a review that provided a taxonomy of IoMT security and privacy issues. Taxonomy helps to identify and understand the threats and vulnerabilities in IoMT environments. Mahmood et al. [68] proposed a comprehensive security model to overcome security threats and attacks in IoMT devices. The developed module identified and prioritized the risks, automatically controlling different levels of threats.

1) BLOCKCHAIN AND DECENTRALISED TECHNOLOGIES IN IoMT SECURITY

Blockchain and decentralized technologies have gained attention as potential solutions for enhancing the security of IoMT systems. These technologies offer immutability, transparency, and decentralized consensus, which can address the security and privacy concerns in IoMT [58]. However, the application of blockchain technology in IoMT security is still an emerging area of research.

Blockchain and decentralized technologies have emerged as potential solutions for enhancing security in IoMT systems. These technologies offer immutability, transparency, and decentralized consensus, which can address security and privacy concerns in IoMT. By leveraging the blockchain, IoMT systems can ensure data integrity, traceability, and secure transactions. Blockchain-enabled IoMT can provide a tamper-resistant and transparent platform for storing and sharing medical data, guaranteeing patient information's authenticity and privacy [69].

In the study by Ktari et al. [70], a platform based on the Internet of Medical Things (IoMT) was proposed for e-health monitoring. The platform utilised smart sensors, such as those that measured blood pressure, Oxygen desatuation, and EEG signals, to collect patient health data. A Blockchain system was employed to ensure the security and confidentiality of information. The collected data were encrypted and relayed through an embedded Raspberry PI4 platform before being processed and stored in an embedded Blockchain node. Preliminary results demonstrated the platform's effectiveness as a low-cost example of a secure Electronic Health Record (EHR) system. This study highlighted the potential of IoMT and Blockchain in revolutionizing healthcare monitoring and data management.

2) ZERO-TRUST FRAMEWORKS FOR SECURING IoMT INFRASTRUCTURE

Zero-trust frameworks have emerged as a promising approach for securing the IoMT infrastructure. These frameworks operate on the principle of not trusting any entity within the network by default, requiring continuous trustworthiness verification [58]. Zero-trust frameworks can help mitigate the risks associated with unauthorized access and lateral movement within IoMT networks.

Zero-trust frameworks can provide granular access control and authentication mechanisms to ensure that only authorized entities can access sensitive medical data. These frameworks can also monitor and analyze network traffic in real-time to detect and respond to potential security threats. IoMT systems can enhance their security posture and protect themselves against internal and external threats by adopting a zero-trust approach.

3) SECURE BOOTSTRAPPING AND FIRMWARE VERIFICATION FOR IoMT DEVICES

Secure bootstrapping and firmware verification are essential to ensure the integrity and security of IoMT devices. Secure bootstrapping involves establishing a trusted initial state for devices, whereas firmware verification ensures that the firmware of the device has not been tampered with [58]. These mechanisms help to prevent unauthorized access and ensure the authenticity of IoMT devices.

During manufacturing, secure bootstrapping involves securely provisioning cryptographic keys and certificates to the IoMT devices. This ensures that only trusted entities can communicate with the devices and that the devices can verify the authenticity of incoming data. Firmware verification involves verifying the integrity and authenticity of the firmware of a device before loading and executing it. This prevents malicious actors from tampering with the firmware and compromises the security of the device.

4) METHODS FOR ANONYMIZING PATIENT DATA IN IoMT

Anonymizing patient data is crucial for protecting the privacy of IoMT systems. Various methods have been proposed for anonymizing patient data while preserving their utility. However, balancing privacy protection and data utility remains challenging [58]. Further research is required to develop effective methods for anonymizing patient data in IoMT environments. Zhao et al. [71] proposed a lightweight privacy-preserving data-sharing scheme for IoMT that ensured patient anonymity and access control. Rajasekaran et al. [72] presented an anonymous authentication protocol based on IoT for secure communication in medical care applications. Wang et al. [73] introduced a cloud-based IoMT data-sharing scheme with conditional anonymous source authentication, which allows patients to share their data with multiple physicians while protecting their identities. A summary of the security and privacy-related work done in IoMT-related areas is presented in TABLE 2.

V. CHALLENGES AND FUTURE DIRECTIONS IN IoMT

This section highlights the major challenges faced during the several stages of the IoMT framework. In addition, potential future directions are recommended for consideration while working on IoMT.

A. CHALLENGES AND OPPORTUNITIES OF IMPLEMENTING ML IN IoMT

The implementation of ML in IoMT can transform healthcare by enhancing diagnostics, treatment, and patient outcomes. However, it must address challenges related to data privacy, quality, diversity, security, processing speed, and ethical considerations, as shown in FIGURE 8, to ensure responsible and effective integration within the healthcare ecosystem. Balancing these challenges with opportunities for improved healthcare delivery and innovation is crucial in shaping the future of IoMT.

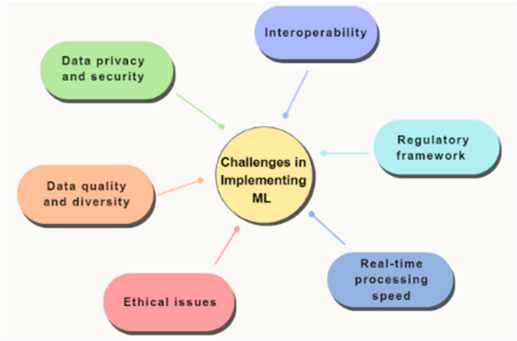
Interoperability
Data privacy and security
Regulatory framework
Challenges in Implementing ML
Data quality and diversity
Real-time processing speed
Ethical issues

FIGURE 8. Challenges implementing ML in IoMT framework.

ML algorithms require large volumes of patient data for training and prediction. However, healthcare data are sensitive and privacy must be ensured to protect against unauthorized access. Furthermore, irregular data quality, including

TABLE 2. Summary of security and privacy related work in IoMT.

Authors	Work proposed	Major Findings	Addressed Threats/Vulnerabilities
Hireche, et al. [74]	The authors explored a range of security strategies and methods which could be applied to tackle the security hurdles within the IoMT framework.	Highlighted the necessity for a multi-tiered security strategy, encompassing access management, verification, data encryption, secure communication protocols, and intrusion detection systems, to safeguard the confidentiality, integrity, and availability of patient data within the IoMT landscape.	Unauthorized Access Data breach
Haseeb, et al. [53]	The authors examined security risks, weaknesses (cyber threats, malicious bots, identity thefts, etc.), and remedial measures for 5G enabled IoMT gadgets.	The digital terrain of IoMT is prone to hacking tactics that can compromise physical security. Ensuring security is pivotal for the successful incorporation of IoMT technology within healthcare infrastructures.	Device Manipulation
Ichikawa, et al. [75]	The authors suggested a Tamper-Proof mobile health technique utilizing Blockchain Technology.	Data collected with the app were stored as JavaScript and sent to the blockchain network. Authors developed a mHealth system for cognitive behavioral therapy using a smartphone app for insomnia.	Unauthorized access
Sun, et al. [58]	The authors explored security and privacy concerns within the IoMT. The downsized IoMT gadgets possess restricted computational capabilities, which poses a challenge in executing sturdy security plans.	Administering and guaranteeing the security of IoMT systems is a tough task, which impedes their utilization for clinical applications.	Identified privacy concerns in IoMT
Shree, et al. [76]	The authors proposed data protection in the IoMT using Blockchain and Secret Sharing Methods.	Formulated an architecture employing a private blockchain and smart contracts for secure gathering, storage, and dissemination of IoMT data.	Unauthorized data access Data breach
Masud, et al. [60]	The authors suggested a lightweight, sturdy, secure key establishment protocol for IoMT in COVID-19 patient care scenarios.	Medical users and vendors possess limited knowledge regarding security threats and potential solutions.	Unauthorized data access
Dai, et al. [69]	The authors proposed Blockchain-Enabled IoMT to combat COVID-19	Deep learning and AI introduce security and privacy vulnerabilities to AI models. Outsourcing IoMT data to cloud servers raises security concerns.	Addressed security and privacy issues
Ahamad & Pathan, 2020	The authors formulated a formally verified authentication protocol within a secure framework for mobile healthcare - COVID-19.	Ensuring the data security and anonymity in cloud-based IoMT settings is a challenge.	Data breach
Almalki, et al. [77]	The authors proposed a preliminary model to integrate blockchain and IoMT for a more thorough analysis of patient health indicators.	Recommended gathering IoMT data via Edge Computing gateway devices and transmitting it to the Cloud Gateway.	Threats and Vulnerabilities were not addressed
Izza, et al. [78]	The authors proposed lightweight authentication schemes for IoMT to ensure secure device communication.	The schemes provide authentication and data integrity while minimizing computational overhead.	Addressed authentication and data integrity issue
Tariq, et al. [79]	The authors explored IoT systems' cybersecurity challenges and vulnerabilities, including IoMT.	Provided insights into potential security threats and future research directions for securing IoT systems.	Threats and Vulnerabilities were not addressed
Al-Turjman and Deebak [80]	The authors suggested a privacy-aware and energy-efficient framework for IoMT in the context of COVID-19.	Addressed the challenges of privacy and energy efficiency in IoMT systems.	Addressed data breach

TABLE 2. ***(Continued.)*** **Summary of security and privacy related work in IoMT.**

Baranchuk, et al. [81]	The authors discussed the cybersecurity considerations for cardiac implantable electronic devices (CIEDs).	Highlighted the importance of protecting CIEDs from potential cyber threats.	Highlighted hacking of medical devices. Addressed device protection
Aman, et al. [82]	The authors surveyed the trends and classification of IoT reviews.	Highlighted the research areas and directions in the field of IoT.	Threats and Vulnerabilities were not addressed
Indumathi, et al. [83]	The authors suggested a blockchain-based IoMT model for uninterrupted and user-friendly healthcare services.	Highlighted the benefits of blockchain technology in ensuring secure and reliable healthcare services.	Addressed Security issues
Ghubaish, et al. [84]	The authors categorized and discussed countermeasures for IoMT security, including authorization, availability, intrusion detection systems, and awareness.	The authors identified open issues and challenges in securing IoMT systems.	Addresses data breach
Pelekoudas-Oikonomou, et al. [3]	The authors reviewed the state-of-the-art blockchain-based security mechanisms for IoMT edge networks.	Offered perspectives on the design and creation of dependable blockchain-based countermeasures for safeguarding IoMT edge networks.	Threats and Vulnerabilities were not addressed
Taherdoost [85]	The authors analyzed blockchain-based IoMT solutions developed between 2017 and 2022.	Highlighted the challenges of scalability in designing blockchain for IoMT systems.	Threats and Vulnerabilities were not addressed
Goel and Neduncheliy an [86]	The authors presented a hybrid Deep Belief-based Diffie Hellman (DBDH) security framework for protecting medical data in IoMT systems.	Utilized a deep belief neural system for continuous monitoring and identification of attacks.	Addresses data breach, security issues
Ksibi, et al. [87]	The authors proposed a system for enhancing trust and decision-making in e-healthcare environments.	Employed an assessment methodology to enhance trust and risk parameters in e-health systems.	Addresses data breach, security issues

noisy data, missing values, and imbalanced data, can hinder the performance of ML algorithms. Hence, ensuring an accurate and reliable approach is a challenge for researchers. In addition, the IoMT framework involves multiple devices and data formats. A major challenge lies in achieving interoperability [88] using ML models that operate seamlessly across the IoMT network.

Further, following regulatory frameworks while implementing ML algorithms using medical data adds complexity, making it challenging for researchers. ML models can reinforce biases in healthcare data, leading to disparities between diagnosis and treatment. Ethical considerations of algorithmic fairness and bias mitigation are essential. Healthcare often requires low-latency responses, particularly for critical applications such as remote monitoring, telemedicine, and surgical robotics. Meeting strict latency requirements is challenging because data processing and transmission delays can have life-threatening consequences. Also, achieving robustness in real-time processing is a great challenge because it involves integrating and incorporating all the challenges shown in FIGURE 8.

As the healthcare industry continues to adopt IoMT, the integration of ML technologies holds immense potential. Researchers can explore and optimize ML algorithms that leverage the vast and complex data generated by IoMT devices to provide more accurate diagnoses, predict disease outcomes, and optimize treatment plans. Personalized medicine, driven by ML algorithms trained on patient-specific data, is likely to become a standard in healthcare, leading to more effective and efficient delivery. Additionally, researchers can enhance the security and privacy aspects of IoMT by developing ML-driven robust methods for protecting sensitive medical data while enabling the seamless flow of information. The ethical implications of ML in IoMT also require attention, necessitating studies on transparency and bias mitigation in ML-driven healthcare systems. However, this involves collaboration between engineers, healthcare experts, and ethicists, shaping a future in which ML-driven IoMT frameworks revolutionize healthcare delivery, making it more precise, accessible, and secure.

B. CHALLENGES AND OPPORTUNITIES OF SECURITY AND PRIVACY IN IoMT

Implementing security and privacy in IoMT remains a complex and evolving challenge, owing to several practical aspects, as shown in FIGURE 9. The IoMT framework consists of a wide range of medical devices with varying levels of complexity, ranging from simple wearables to

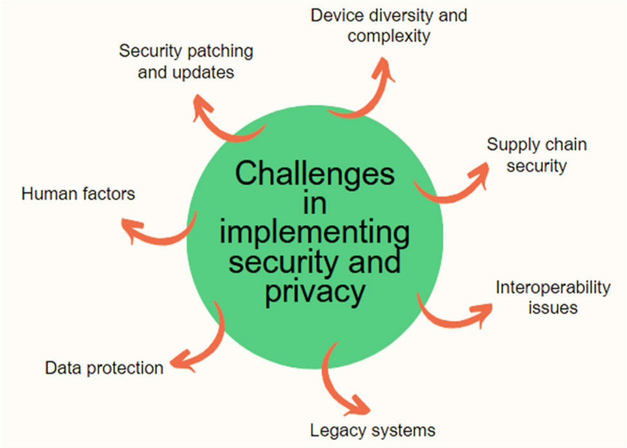
Challenges in implementing security and privacy
Device diversity and complexity
Security patching and updates
Supply chain security
Human factors
Interoperability issues
Data protection
Legacy systems

FIGURE 9. Current challenges of security and privacy in IoMT.

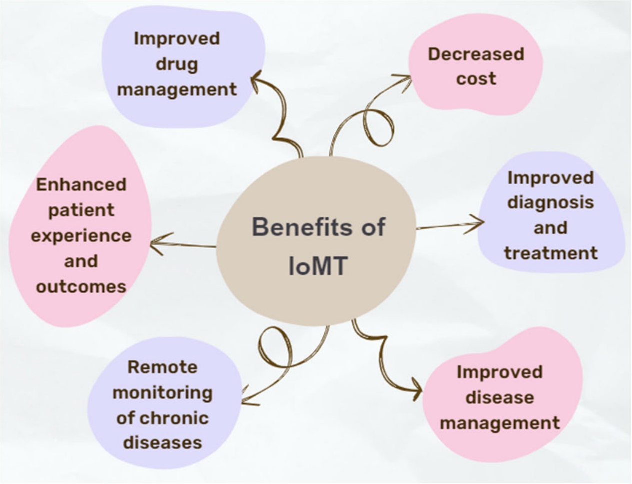
Benefits of IoMT
Improved drug management
Decreased cost
Enhanced patient experience and outcomes
Improved diagnosis and treatment
Remote monitoring of chronic diseases
Improved disease management

FIGURE 10. Benefits of IoMT.

advanced medical instruments leading to device diversity. It is wide array of interconnected medical devices utilized within healthcare systems. These devices form a broad spectrum, including but not limited to wearable health trackers, smart implants, monitoring equipment, diagnostic tools, infusion pumps, and various sensors. Each device serves specific purposes, collects different types of data, and often operates on unique communication protocols. Hence, ensuring consistent security measures across diverse landscapes is a challenge. The challenge arises from integrating these diverse devices seamlessly into a IoMT network. Ensuring interoperability among these devices, allowing them to communicate, share data, and work together efficiently while maintaining data security, privacy, and accuracy poses a significant hurdle in IoMT implementations. Managing this device diversity requires strategies to address compatibility issues, standardize communication protocols, and streamline data integration across various devices to ensure effective and secure operation within the healthcare ecosystem.

In addition, ensuring secure communication between different IoMT devices is essential, but it is a great challenge to achieve with the existing healthcare infrastructure. Additionally, many healthcare facilities still use legacy medical devices that are not designed with modern security, and modernizing the security of these devices can be difficult and costly.

Furthermore, many existing IoMT devices have limited resources and may not support regular security updates, rendering them vulnerable to emerging threats. Patient health data are highly sensitive and are subject to strict privacy regulations. Protecting this data from breaches and unauthorized access is a constant challenge and remains unsatisfactory in real-time scenarios. A great challenge is when healthcare professionals and patients fail to follow the best security practices, leading to vulnerabilities because of a lack of training and awareness. Another issue is ensuring the security of IoMT devices throughout their lifecycle, from manufacturing to disposal. Supply chain attacks can compromise device security. However, these challenges open new avenues for researchers to create opportunities in the future, such as developing robust cutting-edge data protection algorithms, novel encryption methods, secure communication protocols, and intrusion detection systems tailored to the unique challenges IoMT devices and healthcare networks pose. The interdisciplinary nature of IoMT security and privacy allows experts from diverse fields, including computer science, healthcare, and ethics, to collaborate and address complex challenges. This promotes cross-disciplinary research, encouraging fresh perspectives and creative solutions. As IoMT technology continues to evolve, researchers can explore and develop groundbreaking approaches to protect sensitive medical data and foster trust in these systems, ultimately shaping the future of health care security and privacy.

Despite all these challenges, IoMT offers several benefits, as shown in FIGURE 10, which have the potential to transform healthcare on multiple fronts. It enhances patient care by providing real-time monitoring, enabling healthcare providers to remotely track patients' vital signs and health metrics. This continuous data flow allows for early detection of anomalies, enabling timely interventions and improving patient outcomes. IoMT supports telemedicine, bridges geographical gaps, and provides remote access to healthcare services. This is especially crucial in remote areas with limited access to tertiary health centers.

Additionally, IoMT can reduce healthcare costs by preventing hospital readmissions through proactive monitoring and ensuring a more efficient utilization of healthcare resources. Finally, IoMT can support the diseased by giving them superior control over their health and promoting a proactive approach to wellness and self-care. Overall, the benefits of IoMT hold promise for a more patient-centric, efficient, and accessible healthcare system.

Market segmentation is crucial for understanding the diverse landscapes and benefits of IoMT devices. This market can be segmented into various categories based on the

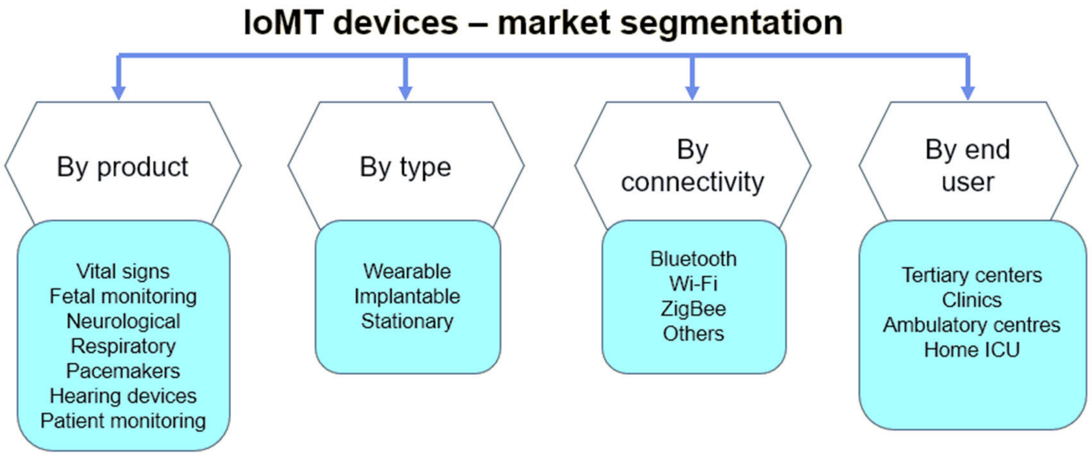

FIGURE 11. IoMT devices market segmentation [91].

TABLE 3. Types of IoMT segments.

Segment	Application
Residential IoMT	Facilitates the transmission of health data from individuals at home to healthcare professionals.
Wearable IoMT	Involves devices worn on the body that monitor health and communicate data to healthcare providers remotely, typically used outside home environments.
Local Community IoMT	Refers to the implementation of IoMT solutions across broader communities or regions for widespread health monitoring.
Healthcare Facility IoMT	Pertains to the use of IoMT technology in clinical and hospital settings, aiding in both healthcare delivery and administrative operations.

types of devices, applications, end users, and geographic regions, as shown in FIGURE 11. The Common device categories include wearable health trackers, medical sensors, implantable devices, and telehealth equipment. Applications include remote patient monitoring, telemedicine, healthcare data analytics, and medication adherence tracking. End users can be categorized as healthcare providers, patients, and healthcare institutions. The end-user segment was categorized into clinics, home care, hospitals, research institutes, academics, and others. In 2022, the hospital segment dominated the market with US$ 17.95 billion revenue (29.16% market share) [89], [90]. This growth is credited to the ever-increasing adoption of remote patient-monitoring systems and EHRs. Geographically, the IoMT market varies in adoption and growth rates across regions and is influenced by factors such as healthcare infrastructure and regulatory environments. Another segmentation is based on connectivity technologies: Bluetooth, Wi-Fi, and Zigbee. Understanding these segments allows researchers to tailor their strategies, target specific markets, and meet the evolving demands of the IoMT framework.

Based on the end-user segment, IoMT can be classified into four types, as listed in TABLE 3. This segmentation helps researchers to develop and optimize algorithms specific to the type to improve efficiency. Each kind demands technological improvements; thus, it becomes less complex than all the segments in one frame. However, security and privacy issues remain unresolved for all types.

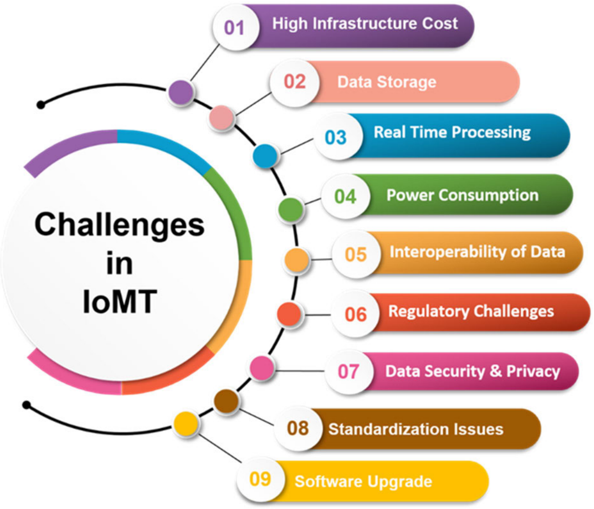

FIGURE 12. Overview of challenges in IoMT.

A demanding network requires various communication protocols to facilitate data exchange between medical devices, sensors, and healthcare systems. These protocols ensure data reliability, security, and interoperability within the health care ecosystem. Some of the different communication IoMT communication standards are outlined in Table 4. researchers who intend to develop or optimize existing protocols can explore the usability and suitability of these protocols in the IoMT framework. However, the choice of

TABLE 4. Different communication protocols in IoMT [74].

Protocol	LoRa WAN	Z-Wave	ZigBee	Sigfox	Bluetooth	IEEE802.11ac
Data Rate (Mbps)	0.0003–0.05 Mbps	0.1 Mbps	0.25 Mbps	1 Mbps	2 Mbps	433–1300 Mbps
Range (m)	20,000 m (rural area), 8,000 m (urban area)	30 m (inside), 100 m (outside)	10–100 m	50,000 m (rural area), 10,000 m (metropolitan area)	10–100 m	35 m (inside), 300 m (outside)
Frequency (GHz)	0.868 GHz (EU), 0.915 GHz (USA)	0.868 GHz (EU), 0.908 GHz (USA)	2.4 GHz	0.868 GHz (EU), 0.902 GHz (USA)	2.4 GHz	5 GHz
Security	AES 128 bits	AES 128 bits	AES 128 bits	Partially addressed	AES 128 bits	WEP-WPA (AES 128 bits)

communication protocol in IoMT depends on factors such as device capabilities, range requirements, power consumption constraints, and specific healthcare applications involved. Selecting an appropriate protocol is essential to ensure a seamless and secure exchange of medical data in IoMT ecosystems.

IoMT has revolutionized healthcare, offering tremendous potential for improved patient care, remote monitoring, and personalized medicine. However, this transformative technology also presents substantial challenges that must be addressed to ensure its successful and secure integration into healthcare systems. The challenges in IoMT are shown in FIGURE 12. based on observations drawn from state-of-the-art methods. These challenges open various avenues for researchers to improve existing systems or invent novel methods to overcome these challenges. Reducing the cost of the entire system is a major challenge; hence, this aspect requires experts to design a cost-efficient framework. This requires the joint effort of researchers from various domains to develop an efficient real-time IoT framework.

VI. CONCLUSION

This research paper reviewed emerging trends, highlighted the technological advancements and challenges within IoMT, and emphasized diverse technological advancements underpinning Smart Healthcare Systems (SHS). This review discussed the evolution of IoMT, Machine Learning Integration, Security, Ethical issues, and the interoperability challenges of IoMT devices. This study reveals that numerous strategies for securing IoMT devices have been published. In addition to security, privacy, and trust, IoMT devices face several challenges. This technology requires an efficient new solution that addresses all security requirements while extending the scope of cyber design. Building a sustainable and power-efficient IoMT-enabled SHS as future healthcare devices is also imperative. Hence, further research studies are needed to concentrate on creating efficient, lightweight intrusion detection systems to protect IoMT-enabled devices.

REFERENCES

[1] F. Alshehri and G. Muhammad, "A comprehensive survey of the Internet of Things (IoT) and AI-based smart healthcare," *IEEE Access*, vol. 9, pp. 3660–3678, 2021, doi: 10.1109/ACCESS.2020.3047960.

[2] J. Silvestre-Blanes, V. Sempere-Payá, and T. Albero-Albero, "Smart sensor architectures for multimedia sensing in IoMT," *Sensors*, vol. 20, no. 5, p. 1400, Mar. 2020, doi: 10.3390/s20051400.

[3] F. Pelekoudas-Oikonomou, G. Zachos, M. Papaioannou, M. de Ree, J. C. Ribeiro, G. Mantas, and J. Rodriguez, "Blockchain-based security mechanisms for IoMT edge networks in IoMT-based healthcare monitoring systems," *Sensors*, vol. 22, no. 7, p. 2449, Mar. 2022, doi: 10.3390/s22072449.

[4] T. Adenaiye, W. Bul'ajoul, and F. Olajide, "Security performance of Internet of Medical Things," *Adv. Netw.*, vol. 9, no. 1, p. 1, 2021, doi: 10.11648/j.net.20210901.11.

[5] R. John Martin, "IoMT supported COVID care—Technologies and challenges," *Int. J. Eng. Manage. Res.*, vol. 12, no. 1, pp. 125–131, Feb. 2022.

[6] F. Alsubaei, A. Abuhussein, and S. Shiva, "Ontology-based security recommendation for the Internet of Medical Things," *IEEE Access*, vol. 7, pp. 48948–48960, 2019, doi: 10.1109/ACCESS.2019.2910087.

[7] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop, J. Rodriguez, and D. Lymberopoulos, "A survey on security threats and countermeasures in Internet of Medical Things (IoMT)," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 6, p. e4049, Jun. 2022.

[8] F. P. Oikonomou, J. Ribeiro, G. Mantas, J. M. C. S. Bastos, and J. Rodriguez, "A hyperledger fabric-based blockchain architecture to secure iot-based health monitoring systems," in *Proc. IEEE Int. Medit. Conf. Commun. Netw. (MeditCom)*, Sep. 2021, pp. 186–190, doi: 10.1109/MeditCom49071.2021.9647521.

[9] F. P. Oikonomou, G. Mantas, P. Cox, F. Bashashi, F. Gil-Castiñeira, and J. Gonzalez, "A blockchain-based architecture for secure IoT-based health monitoring systems," in *Proc. IEEE 26th Int. Workshop Comput. Aided Model. Design Commun. Links Netw. (CAMAD)*, Oct. 2021, pp. 1–6, doi: 10.1109/CAMAD52502.2021.9617803.

[10] D. Shin and Y. Hwang, "Integrated acceptance and sustainability evaluation of Internet of Medical Things: A dual-level analysis," *Internet Res.*, vol. 27, no. 5, pp. 1227–1254, Oct. 2017.

[11] M. I. Tariq, N. A. Mian, A. Sohail, T. Alyas, and R. Ahmad, "Evaluation of the challenges in the Internet of Medical Things with multicriteria decision making (AHP and TOPSIS) to overcome its obstruction under fuzzy environment," *Mobile Inf. Syst.*, vol. 2020, pp. 1–19, Aug. 2020.

[12] M. Javaid, A. Haleem, R. P. Singh, R. Suman, and S. Rab, "Significance of machine learning in healthcare: Features, pillars and applications," *Int. J. Intell. Netw.*, vol. 3, pp. 58–73, Jan. 2022.

[13] Y. Kumar, A. Koul, R. Singla, and M. F. Ijaz, "Artificial intelligence in disease diagnosis: A systematic literature review, synthesizing framework and future research agenda," *J. Ambient Intell. Humanized Comput.*, vol. 2022, pp. 1–28, Jan. 2022.

[14] P. Manickam, S. A. Mariappan, S. M. Murugesan, S. Hansda, A. Kaushik, R. Shinde, and S. P. Thipperudraswamy, "Artificial intelligence (AI) and Internet of Medical Things (IoMT) assisted biomedical systems for intelligent healthcare," *Biosensors*, vol. 12, no. 8, p. 562, Jul. 2022, doi: 10.3390/bios12080562.

[15] N. Nigar, A. Jaleel, S. Islam, M. K. Shahzad, and E. A. Affum, "IoMT meets machine learning: From edge to cloud chronic diseases diagnosis system," *J. Healthcare Eng.*, vol. 2023, pp. 1–13, Jun. 2023, doi: 10.1155/2023/9995292.

[16] F. Dahan, R. Alroobaea, W. Y. Alghamdi, M. K. Mohammed, F. Hajjej, D. M. Alsekait, and K. Raahemifar, ''A smart IoMT based architecture for E-healthcare patient monitoring system using artificial intelligence algorithms,'' *Frontiers Physiol.*, vol. 14, Jan. 2023, Art. no. 1125952, doi: 10.3389/fphys.2023.1125952.

[17] E. Yildirim, M. Cicioglu, and A. Çalhan, ''Real-time Internet of Medical Things framework for early detection of COVID-19,'' *Neural Comput. Appl.*, vol. 34, no. 22, pp. 20365–20378, Nov. 2022.

[18] S. Thandapani, M. I. Mahaboob, C. Iwendi, D. Selvaraj, A. Dumka, M. Rashid, and S. Mohan, ''IoMT with deep CNN: AI-based intelligent support system for pandemic diseases,'' *Electronics*, vol. 12, no. 2, p. 424, Jan. 2023.

[19] A. J. D. Krupa, S. Dhanalakshmi, K. W. Lai, Y. Tan, and X. Wu, ''An IoMT enabled deep learning framework for automatic detection of fetal QRS: A solution to remote prenatal care,'' *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 9, pp. 7200–7211, Oct. 2022, doi: 10.1016/j.jksuci.2022.07.002.

[20] P. Emee Dutta, H. Neog, and N. Medhi, ''Health monitoring in Internet of Medical Things (IoMT) using machine learning (ML) approaches,'' in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2021, pp. 1–6, doi: 10.1109/GCWkshps52748.2021.9682039.

[21] N. Bibi, M. Sikandar, I. Ud Din, A. Almogren, and S. Ali, ''IoMT-based automated detection and classification of leukemia using deep learning,'' *J. Healthcare Eng.*, vol. 2020, pp. 1–12, Dec. 2020, doi: 10.1155/2020/6648574.

[22] A. Sampathkumar, M. Tesfayohani, S. K. Shandilya, S. B. Goyal, S. S. Jamal, P. K. Shukla, P. Bedi, and M. Albeedan, ''Internet of Medical Things (IoMT) and reflective belief design-based big data analytics with convolution neural network-metaheuristic optimization procedure (CNN-MOP),'' *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–14, Mar. 2022.

[23] M. F. Khan, T. M. Ghazal, R. A. Said, A. Fatima, S. Abbas, M. A. Khan, G. F. Issa, M. Ahmad, and M. A. Khan, ''An IoMT-enabled smart healthcare model to monitor elderly people using machine learning technique,'' *Comput. Intell. Neurosci.*, vol. 2021, pp. 1–10, Nov. 2021, doi: 10.1155/2021/2487759.

[24] M. Jarrah, H. Al Hamadi, A. Abu-Khadrah, and T. M. Ghazal, ''IoMT-based smart healthcare of elderly people using deep extreme learning machine,'' *Comput., Mater. Continua*, vol. 76, no. 1, pp. 19–33, 2023.

[25] A. L. N. Al-hajjar and A. K. M. Al-Qurabat, ''An overview of machine learning methods in enabling IoMT-based epileptic seizure detection,'' *J. Supercomput.*, vol. 79, no. 14, pp. 16017–16064, Apr. 2023, doi: 10.1007/s11227-023-05299-9.

[26] L. Rachakonda, P. Rajkumar, S. P. Mohanty, and E. Kougianos, ''IMirror: A smart mirror for stress detection in the IoMT framework for advancements in smart cities,'' in *Proc. IEEE Int. Smart Cities Conf. (ISC)*, Sep. 2020, pp. 1–7, doi: 10.1109/ISC251055.2020.9239081.

[27] C. Iwendi, S. Khan, J. H. Anajemba, A. K. Bashir, and F. Noor, ''Realizing an efficient IoMT-assisted patient diet recommendation system through machine learning model,'' *IEEE Access*, vol. 8, pp. 28462–28474, 2020, doi: 10.1109/ACCESS.2020.2968537.

[28] E. Elbasi and A. I. Zreikat, ''Efficient early prediction and diagnosis of diseases using machine learning algorithms for IoMT data,'' in *Proc. IEEE World AI IoT Congr. (AIIoT)*, May 2021, pp. 0155–0159, doi: 10.1109/AIIoT52608.2021.9454231.

[29] A. Kumar, K. Sharma, and A. Sharma, ''Genetically optimized fuzzy C-means data clustering of IoMT-based biomarkers for fast affective state recognition in intelligent edge analytics,'' *Appl. Soft Comput.*, vol. 109, Sep. 2021, Art. no. 107525, doi: 10.1016/j.asoc.2021.107525.

[30] P. Tiwari, A. Lakhan, R. H. Jhaveri, and T.-M. Gronli, ''Consumer-centric Internet of Medical Things for cyborg applications based on federated reinforcement learning,'' *IEEE Trans. Consum. Electron.*, early access, Feb. 7, 2023, doi: 10.1109/TCE.2023.3242375.

[31] S. A. Wagan, J. Koo, I. F. Siddiqui, M. Attique, D. R. Shin, and N. M. F. Qureshi, ''Internet of Medical Things and trending converged technologies: A comprehensive review on real-time applications,'' *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 10, pp. 9228–9251, Nov. 2022, doi: 10.1016/j.jksuci.2022.09.005.

[32] D. Gupta, M. Bhatia, and A. Kumar, ''Real-time mental health analytics using IoMT and social media datasets: Research and challenges,'' in *Proc. Int. Conf. Innov. Comput. Commun. (ICICC)*, 2021, doi: 10.2139/ssrn.3842818.

[33] P. Raj, J. M. Chatterjee, A. Kumar, and B. Balamurugan, *Internet of Things Use Cases for the Healthcare Industry*. Berlin, Germany: Springer, 2020.

[34] O. Debauche, J. B. Nkamla Penka, S. Mahmoudi, X. Lessage, M. Hani, P. Manneback, U. K. Lufuluabu, N. Bert, D. Messaoudi, and A. Guttadauria, ''RAMi: A new real-time Internet of Medical Things architecture for elderly patient monitoring,'' *Information*, vol. 13, no. 9, p. 423, Sep. 2022.

[35] A. A. Aljabr and K. Kumar, ''Design and implementation of Internet of Medical Things (IoMT) using artificial intelligent for mobile-healthcare,'' *Meas., Sensors*, vol. 24, Dec. 2022, Art. no. 100499.

[36] M. W. Bhatt and S. Sharma, ''An IoMT-based approach for real-time monitoring using wearable neuro-sensors,'' *J. Healthcare Eng.*, vol. 2023, pp. 1–10, Feb. 2023, doi: 10.1155/2023/1066547.

[37] S. Nickolas and K. Shobha, ''Efficient pre-processing techniques for improving classifiers performance,'' *J. Web Eng.*, vol. 21, pp. 203–228, Dec. 2021.

[38] C. Fan, M. Chen, X. Wang, J. Wang, and B. Huang, ''A review on data preprocessing techniques toward efficient and reliable knowledge discovery from building operational data,'' *Frontiers Energy Res.*, vol. 9, Mar. 2021, Art. no. 652801.

[39] A. Islam, S. Seth, T. Bhadra, S. Mallik, A. Roy, A. Li, and M. Sarkar, ''Feature selection, clustering and IOMT on biomedical engineering for COVID-19 pandemic: A comprehensive review,'' *J. Data Sci. Intell. Syst.*, Jun. 2023, doi: 10.47852/bonviewJDSIS3202916.

[40] M. L. Hernandez-Jaimes, A. Martinez-Cruz, K. A. Ramírez-Gutiérrez, and C. Feregrino-Uribe, ''Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and cloud-fog-edge architectures,'' *Internet Things*, vol. 23, Oct. 2023, Art. no. 100887.

[41] Y. Rbah, M. Mahfoudi, Y. Balboul, M. Fattah, S. Mazer, M. Elbekkali, and B. Bernoussi, ''Machine learning and deep learning methods for intrusion detection systems in IoMT: A survey,'' in *Proc. 2nd Int. Conf. Innov. Res. Appl. Sci., Eng. Technol. (IRASET)*, Mar. 2022, pp. 1–9.

[42] M. Alalhareth and S.-C. Hong, ''An improved mutual information feature selection technique for intrusion detection systems in the Internet of Medical Things,'' *Sensors*, vol. 23, no. 10, p. 4971, May 2023, doi: 10.3390/s23104971.

[43] P. K. R. Maddikunta, M. Parimala, S. Koppu, T. R. Gadekallu, C. L. Chowdhary, and M. Alazab, ''An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture,'' *Comput. Commun.*, vol. 160, pp. 139–149, Jul. 2020, doi: 10.1016/j.comcom.2020.05.048.

[44] G. Thamilarasu, A. Odesile, and A. Hoang, ''An intrusion detection system for Internet of Medical Things,'' *IEEE Access*, vol. 8, pp. 181560–181576, 2020.

[45] S. Saif, N. Yasmin, and S. Biswas, ''Feature engineering based performance analysis of ML and DL algorithms for botnet attack detection in IoMT,'' *Int. J. Syst. Assurance Eng. Manag.*, vol. 14, no. 1, pp. 512–522, Mar. 2023.

[46] A. Binbusayyis, H. Alaskar, T. Vaiyapuri, and M. Dinesh, ''An investigation and comparison of machine learning approaches for intrusion detection in IoMT network,'' *J. Supercomput.*, vol. 78, no. 15, pp. 17403–17422, Oct. 2022.

[47] Z. Guan, Z. Lv, X. Du, L. Wu, and M. Guizani, ''Achieving data utility-privacy tradeoff in Internet of Medical Things: A machine learning approach,'' *Future Gener. Comput. Syst.*, vol. 98, pp. 60–68, Sep. 2019, doi: 10.1016/j.future.2019.01.058.

[48] Z. Guan, Y. Li, S. Yu, and Z. Yang, ''Deep reinforcement learning-based full-duplex link scheduling in federated learning-based computing for IoMT,'' *Trans. Emerg. Telecommun. Technol.*, vol. 34, no. 3, p. e4724, Mar. 2023.

[49] M. Soleimani and A. S. Mirshahzadeh, ''Multi-class classification of imbalanced intelligent data using deep neural network,'' *EAI Endorsed Trans. AI Robot.*, vol. 2, pp. 1–10, Jul. 2023.

[50] Y. J. Ha, G. Lee, M. Yoo, S. Jung, S. Yoo, and J. Kim, ''Feasibility study of multi-site split learning for privacy-preserving medical systems under data imbalance constraints in COVID-19, X-ray, and cholesterol dataset,'' *Sci. Rep.*, vol. 12, no. 1, p. 1534, Jan. 2022, doi: 10.1038/s41598-022-05615-y.

[51] M. Sugadev, S. J. Rayen, J. Harirajkumar, R. Rathi, G. Anitha, S. Ramesh, and K. Ramaswamy, ''Implementation of combined machine learning with the big data model in IoMT systems for the prediction of network resource consumption and improving the data delivery,'' *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–12, Jul. 2022.

[52] N. J. Ali, N. A. Hamzah, A. M. Ali, P. S. JosephNg, J. F. Tawfeq, and A. D. Radhi, "An intelligent approach for enhancing the quality of service in IoMT based on 5G," *Periodicals Eng. Natural Sci. (PEN)*, vol. 11, no. 3, pp. 58–67, May 2023.

[53] K. Haseeb, I. Ahmad, I. I. Awan, J. Lloret, and I. Bosch, "A machine learning SDN-enabled big data model for IoMT systems," *Electronics*, vol. 10, no. 18, p. 2228, Sep. 2021.

[54] A. Nazari, M. Kordabadi, R. Mohammadi, and C. Lal, "EQRSRL: An energy-aware and QoS-based routing schema using reinforcement learning in IoMT," *Wireless Netw.*, vol. 29, no. 7, pp. 3239–3253, Oct. 2023.

[55] B. Priya and J. Malhotra, "IMnet: Intelligent RAT selection framework for 5G enabled IoMT network," *Wireless Pers. Commun.*, vol. 129, no. 2, pp. 911–932, Mar. 2023.

[56] L. Rachakonda, S. P. Mohanty, and E. Kougianos, "ILog: An intelligent device for automatic food intake monitoring and stress detection in the IoMT," *IEEE Trans. Consum. Electron.*, vol. 66, no. 2, pp. 115–124, May 2020, doi: 10.1109/TCE.2020.2976006.

[57] A. A. Toor, M. Usman, F. Younas, A. C. M. Fong, S. A. Khan, and S. Fong, "Mining massive e-health data streams for IoMT enabled healthcare systems," *Sensors*, vol. 20, no. 7, p. 2131, Apr. 2020, doi: 10.3390/s20072131.

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

[59] T. Ahmed Alhaj, S. M. Abdulla, M. A. E. Iderss, A. A. A. Ali, F. A. Elhaj, M. A. Remli, and L. A. Gabralla, "A survey: To govern, protect, and detect security principles on Internet of Medical Things (IoMT)," *IEEE Access*, vol. 10, pp. 124777–124791, 2022, doi: 10.1109/ACCESS.2022.3225038.

[60] M. Masud, G. S. Gaba, S. Alqahtani, G. Muhammad, B. B. Gupta, P. Kumar, and A. Ghoneim, "A lightweight and robust secure key establishment protocol for Internet of Medical Things in COVID-19 patients care," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15694–15703, Nov. 2021, doi: 10.1109/JIOT.2020.3047662.

[61] M. Hamza, M. A. Akbar, M. Shafiq, T. Kamal, and A. M. Baddour, "Identification of privacy and security risks of Internet of Things: An empirical investigation," *Rev. Comput. Eng. Res.*, vol. 6, no. 1, pp. 35–44, 2019.

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

[63] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, vol. 107, pp. 841–853, Jun. 2020, doi: 10.1016/j.future.2017.08.020.

[64] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *Proc. 52nd ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, Jun. 2015, pp. 1–6.

[65] M. K. Hasan, T. M. Ghazal, R. A. Saeed, B. Pandey, H. Gohel, A. A. Eshmawi, S. Abdel-Khalek, and H. M. Alkhassawneh, "A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things," *IET Commun.*, vol. 16, no. 5, pp. 421–432, Mar. 2022.

[66] D. S. Gupta, N. Mazumdar, A. Nag, and J. P. Singh, "Secure data authentication and access control protocol for industrial healthcare system," *J. Ambient Intell. Humanized Comput.*, vol. 14, no. 5, pp. 4853–4864, May 2023.

[67] P. A. H. Williams and V. McCauley, "Always connected: The security challenges of the healthcare Internet of Things," in *Proc. IEEE 3rd World Forum Internet Things (WF-IoT)*, Dec. 2016, pp. 30–35, doi: 10.1109/WF-IoT.2016.7845455.

[68] M. Mahmood, M. I. Khan, H. Hussain, I. Khan, S. Rahman, M. Shabir, and B. Niazi, "Improving security architecture of Internet of Medical Things: A systematic literature review," *IEEE Access*, vol. 11, pp. 107725–107753, 2023, doi: 10.1109/ACCESS.2023.3281655.

[69] H.-N. Dai, M. Imran, and N. Haider, "Blockchain-enabled Internet of Medical Things to combat COVID-19," *IEEE Internet Things Mag.*, vol. 3, no. 3, pp. 52–57, Sep. 2020, doi: 10.1109/IOTM.0001.2000087.

[70] J. Ktari, T. Frikha, N. B. Amor, L. Louraidh, H. Elmannai, and M. Hamdi, "IoMT-based platform for e-health monitoring based on the blockchain," *Electronics*, vol. 11, no. 15, p. 2314, Jul. 2022. [Online]. Available: https://www.mdpi.com/2079-9292/11/15/2314

[71] Z. Zhao, C. Hsu, L. Harn, Q. Yang, and L. Ke, "Lightweight privacy-preserving data sharing scheme for Internet of Medical Things," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–13, Sep. 2021, doi: 10.1155/2021/8402138.

[72] A. S. Rajasekaran, D. Yuvaraj, and A. Maria, "Secure authentication scheme for medical care applications based on IoT," in *Proc. Int. Conf. Emerging Smart Comput. Inform. (ESCI)*, Mar. 2022, pp. 1–5, doi: 10.1109/ESCI53509.2022.9758235.

[73] Y.-P. Wang, X.-F. Wang, H.-N. Dai, X.-S. Zhang, Y. Su, M. Imran, and N. Nasser, "A cloud-based IoMT data sharing scheme with conditional anonymous source authentication," in *Proc. IEEE Global Commun. Conf.*, Dec. 2022, pp. 2915–2920, doi: 10.1109/GLOBECOM48099.2022.10000912.

[74] R. Hireche, H. Mansouri, and A.-S.-K. Pathan, "Security and privacy management in Internet of Medical Things (IoMT): A synthesis," *J. Cybersecurity Privacy*, vol. 2, no. 3, pp. 640–661, Aug. 2022.

[75] D. Ichikawa, M. Kashiyama, and T. Ueno, "Tamper-resistant mobile health using blockchain technology," *JMIR mHealth uHealth*, vol. 5, no. 7, p. e111, Jul. 2017, doi: 10.2196/mhealth.7938.

[76] S. Shree, C. Zhou, and M. Barati, "Data protection in Internet of Medical Things using blockchain and secret sharing method," *J. Supercomput.*, doi: 10.1007/s11227-023-05657-7.

[77] J. Almalki, W. Al Shehri, R. Mehmood, K. Alsaif, S. M. Alshahrani, N. Jannah, and N. A. Khan, "Enabling blockchain with IoMT devices for healthcare," *Information*, vol. 13, no. 10, p. 448, Sep. 2022. [Online]. Available: https://www.mdpi.com/2078-2489/13/10/448

[78] S. Izza, F. Merazka, and M. Benssalah, "Lightweight authentication schemes for Internet of Medical Things," in *Proc. 2nd Int. Conf. Adv. Electr. Eng. (ICAEE)*, Oct. 2022, pp. 1–6, doi: 10.1109/ICAEE53772.2022.9962096.

[79] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review," *Sensors*, vol. 23, no. 8, p. 4117, Apr. 2023, doi: 10.3390/s23084117.

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

[81] A. Baranchuk, M. M. Refaat, K. K. Patton, M. K. Chung, K. Krishnan, V. Kutyifa, G. Upadhyay, J. D. Fisher, and D. R. Lakkireddy, "Cybersecurity for cardiac implantable electronic devices," *J. Amer. College Cardiol.*, vol. 71, no. 11, pp. 1284–1288, Mar. 2018, doi: 10.1016/j.jacc.2018.01.023.

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

[83] J. Indumathi, A. Shankar, M. R. Ghalib, J. Gitanjali, Q. Hua, Z. Wen, and X. Qi, "Block chain based Internet of Medical Things for uninterrupted, ubiquitous, user-friendly, unflappable, unblemished, unlimited health care services (BC IoMT u6 HCS)," *IEEE Access*, vol. 8, pp. 216856–216872, 2020, doi: 10.1109/ACCESS.2020.3040240.

[84] 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.

[85] H. Taherdoost, "Blockchain-based Internet of Medical Things," *Appl. Sci.*, vol. 13, no. 3, p. 1287, Jan. 2023. [Online]. Available: https://www.mdpi.com/2076-3417/13/3/1287

[86] A. Goel and S. Neduncheliyan, "An intelligent blockchain strategy for decentralised healthcare framework," *Peer-Peer Netw. Appl.*, vol. 16, no. 2, pp. 846–857, Mar. 2023, doi: 10.1007/s12083-022-01429-x.

[87] A. Ksibi, H. Mhamdi, M. Ayadi, L. Almuqren, M. S. Alqahtani, M. D. Ansari, A. Sharma, and S. Hedi, "Secure and fast emergency road healthcare service based on blockchain technology for smart cities," *Sustainability*, vol. 15, no. 7, p. 5748, Mar. 2023. [Online]. Available: https://www.mdpi.com/2071-1050/15/7/5748

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

[89] J. B. Awotunde, M. F. Ijaz, A. K. Bhoi, M. AbdulRaheem, I. D. Oladipo, and P. Barsocchi, "Edge-IoMT-based enabled architecture for smart healthcare system," in *5G IoT Edge Comput. for Smart Healthcare*. Amsterdam, The Netherlands: Elsevier, 2022, pp. 1–27.

[90] A. Sinha, D. W. Garcia, B. Kumar, and P. Banerjee, "Application of big data analytics and Internet of Medical Things (IoMT) in healthcare with view of explainable artificial intelligence: A survey," in *Interpretable Cognitive Internet of Things for Healthcare*. Berlin, Germany: Springer, 2023, pp. 129–163.

[91] T. Shakeel, S. Habib, W. Boulila, A. Koubaa, A. R. Javed, M. Rizwan, T. R. Gadekallu, and M. Sufiyan, "A survey on COVID-19 impact in the healthcare domain: Worldwide market implementation, applications, security and privacy issues, challenges and future prospects," *Complex Intell. Syst.*, vol. 9, no. 1, pp. 1027–1058, Feb. 2023.

G. R. PRADYUMNA received the B.E. degree in telecommunication engineering and the M.Tech. degree in digital electronics and communication, in 2005 and 2009, respectively. He is currently pursuing the Ph.D. degree with the National Institute of Technology, Surathkal, Karnataka, India. He is also an Assistant Professor with the Department of Electronics and Communication Engineering, N.M.A.M. Institute of Technology, Udupi, India. His areas of interests include cryptography, embedded systems, the IoT, and HDL.

ROOPA B. HEGDE received the B.E. degree in telecommunication engineering and the M.Tech. degree in digital electronics and communication, in 2005 and 2009, respectively, and the Ph.D. degree from MSIS, Manipal, Karnataka, India, in 2020. Currently, she is an Associate Professor with the Department of Electronics and Communication Engineering, N.M.A.M. Institute of Technology, Udupi, India. She has published several articles in peer-reviewed journals. Her areas of interests include digital electronics, image processing, pattern recognition, artificial intelligence, and machine learning.

K. B. BOMMEGOWDA received the B.E. degree in electronics and communication engineering, the M.Tech. degree in industrial electronics, and the Ph.D. degree in polymer composites from Visvesvaraya Technological University, Belagavi, Karnataka, in 2010, 2015, and 2022, respectively. He is currently an Assistant Professor with the Department of Electronics and Communication Engineering, N.M.A.M. Institute of Technology, Udupi, India. His area of interests include nano dielectrics and insulation systems, control systems, power electronics, and healthcare devices.

TONY JAN is currently the Head of the School of IT and the Director of the Artificial Intelligence Research Centre, Torrens University, Australia. Previously, he was the Associate Head and an Associate Professor with the School of IT and Engineering, Melbourne Institute of Technology, and the University of Technology Sydney, respectively. He specializes in machine learning for cybersecurity and smart technologies, with over 70 articles in prestigious journals, supported by several large research grants totaling over 20 million dollars in the domains of AI automation and homeland security.

GANESH R. NAIK received the Ph.D. degree in electronics engineering, specializing in biomedical engineering and signal processing from RMIT University, Melbourne, Australia, in December 2009. He is a leading expert in data science and biomedical signal processing. Currently, he is a Senior Lecturer of IT and CS with Torrens University, Adelaide, Australia. Previously, he was an Academic and Research Theme Co-Lead with the Flinders University's Sleep Institute. He was a Postdoctoral Research Fellow with the MARCS Institute, Western Sydney University, from July 2017 to July 2020. Before that, he was a Chancellor's Postdoctoral Research Fellow with the Centre for Health Technologies, University of Technology Sydney (UTS), from February 2013 to June 2017. As a mid-career researcher, he has edited 14 books and authored around 150 papers in peer-reviewed journals and conferences. He ranked top 2% of researchers worldwide in biomedical engineering. He was a Baden–Württemberg Scholarship recipient from Berufsakademie, Stuttgart, Germany, from 2006 to 2007. In 2010, he received the ISSI Overseas Fellowship from Skilled Institute Victoria, Australia. Recently, he received the BridgeTech Industry Fellowship from the Medical Research Future Fund, Government of Australia. He is an Associate Editor of IEEE ACCESS, *Frontiers in Neurorobotics*, and two Springer journals.