IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 9 November 2023, accepted 17 January 2024, date of publication 26 January 2024, date of current version 14 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3358827

TOPICAL REVIEW

A Review on the Application of Internet of Medical Things in Wearable Personal Health Monitoring: A Cloud-Edge Artificial Intelligence Approach

KARISMA TRINANDA PUTRA[1,2,3], (Member, IEEE), AHMAD ZAKI ARRAYYAN[1,2,4], NUR HAYATI[1,2], (Member, IEEE), FIRDAUS[4], (Member, IEEE), CAHYA DAMARJATI[5], (Member, IEEE), ABU BAKAR[6], AND HSING-CHUNG CHEN[7,8], (Senior Member, IEEE)

[1]Department of Electrical Engineering, Faculty of Engineering, Universitas Muhammadiyah Yogyakarta, Bantul 55183, Indonesia
[2]Center of Artificial Intelligence and Robotics Studies, Research and Innovation Centre, Universitas Muhammadiyah Yogyakarta, Bantul 55183, Indonesia
[3]Center for AI and Cyber Security Research and Innovations, Asia University, Taichung City 41354, Taiwan
[4]Department of Electrical Engineering, Faculty of Industrial Technology, University Islam Indonesia, Sleman 55584, Indonesia
[5]Department of Information Technology, Faculty of Engineering, Universitas Muhammadiyah Yogyakarta, Bantul 55183, Indonesia
[6]Department of Oral Medicine, Faculty of Dentistry, Baiturrahmah University, Padang 25176, Indonesia
[7]Department of Computer Science and Information Engineering, College of Information and Electrical Engineering, Asia University, Taichung City 413305, Taiwan
[8]Department of Medical Research, China Medical University Hospital, China Medical University, Taichung City 404328, Taiwan

Corresponding authors: Hsing-Chung Chen (shin8409@ms6.hinet.net) and Karisma Trinanda Putra (karisma@ft.umy.ac.id)

This work was supported in part by Universitas Muhammadiyah Yogyakarta, Indonesia through the Center of Artificial Intelligence and Robotic Studies, the Research and Innovation Centre, under grant number 50/R-LRI/XII/2023 and the Cooperation and International Affairs under grant number 0108/A.3-VIII/X/2023. This study was partly carried out under the Matching Fund Program by the Ministry of Education, Culture, Research, and Technology, Indonesia under grant number 0540/E/KS.06.02/2022. This work was also supported by the Chelpis Quantum Tech Co., Ltd., Taiwan, under grant number Asia University: I112IB120. This work was also supported in part by Asia University, Taiwan, and China Medical University Hospital, China Medical University, Taiwan, under grant numbers ASIA-111-CMUH-16, ASIA-110-CMUH-22, ASIA108-CMUH-05, ASIA-106-CMUH-04, and ASIA-105-CMUH-04.

ABSTRACT The advent of the fifth-generation mobile communication technology (5G) era has catalyzed significant advancements in medical diagnosis delivery, primarily driven by the surge in medical data from wearable Internet of Medical Things (IoMT) devices. Nonetheless, the IoMT paradigm grapples with challenges related to data security, privacy, constrained computational capabilities at the edge, and an inadequate architecture for handling traditionally error-prone data. In this context, our research offers: (1) an exhaustive review of large-scale medical data propelled by IoMT, (2) an exploration of the prevailing cloud-edge Artificial Intelligence (AI) framework tailored for IoMT, and (3) an insight into the application of Edge Federated Learning (EFL) in bolstering medical big data analytics to yield secure and superior diagnostic outcomes. We place a particular emphasis on the proliferation of IoMT wearable devices that incessantly stream medical data, either from patients or healthcare institutions, to centralized repositories. Furthermore, we introduce a federated cloud-edge AI blueprint designed to position computational resources proximate to the edge network, facilitating real-time diagnostic feedback to patients. We conclude by delineating prospective research trajectories in enhancing IoMT through AI integration.

INDEX TERMS Wearable Internet of Medical Things, cloud-edge AI, edge federated learning.

I. INTRODUCTION

Although the medical industry embarked on its digital transformation earlier than many sectors, its progression has been

The associate editor coordinating the review of this manuscript and approving it for publication was Roberto C. Ambrosio.

notably gradual [1]. Rapid strides in science, technology, and economic landscapes have thrust healthcare into the limelight, capturing personal, societal, and national interests. Traditional medical practices grapple with challenges such as prohibitive treatment costs, hurdles in securing doctor consultations, and opacity in medical data dissemination [2]. Since its formal inception in 1999, the Internet of Things (IoT) has permeated every dimension of the contemporary Internet of Everything (IoE) era [3]. Advanced IoT frameworks, exemplified by the Internet of Medical Things (IoMT), have been synergistically integrated with smartphones, wireless protocols, and diverse devices, fostering seamless interconnectivity between patients, medical professionals, healthcare institutions, and medical equipment [4]. Positioned at the nexus of the medical sector's digital metamorphosis, IoMT, inclusive of wearable technologies, epitomizes the specialized application of IoT paradigms in healthcare.

Wearable devices, encompassing smartwatches, fitness trackers, and specialized medical sensors, serve as pivotal elements within the IoMT landscape, facilitating real-time vital sign monitoring, comprehensive patient health data acquisition, and the provision of remote healthcare services [5]. These devices continuously relay data, granting healthcare practitioners profound insights into patient health, thereby paving the way for tailored medical interventions. The assimilation of wearables within the IoMT infrastructure empowers healthcare systems to leverage interconnected technologies, thereby elevating patient care standards, refining diagnostic accuracy, and transforming healthcare service delivery. Central to this interconnected matrix is the wireless healthcare sensor. A robust wireless sensor network, comprising diverse sensor types such as pressure, biological, and embedded sensors, is indispensable for the meticulous collection of patient vital statistics. Presently, sensors are ubiquitously employed in settings like operating rooms, emergency departments, and intensive care units (ICU) to capture and relay critical patient states. Moreover, wearable health devices, anchored by sensors, transcend temporal and spatial constraints, enabling real-time patient monitoring [6], substantially reducing treatment expenses, and ensuring patients access bespoke medical care at their convenience.

Recent studies suggest that the advent of 5G mobile communication technology is poised to profoundly influence the evolution of the medical sector [7]. Digital medical applications, encompassing remote consultations, surgical mentorship, emergency response vehicles, and wearable medical instruments, are projected to gain more traction. Concurrently, there will be a diversification in the cadre of developers crafting applications harnessing 5G capabilities, and their populace is set to burgeon [8]. It is crucial to process, evaluate, and make decisions about the gathered medical data rapidly and in real time since it directly affects patients' health and quality of life. However, the rapid and real-time gathering of medical data increases the risk of exposing sensitive information and compromising patient privacy. Consequently, the stringent policies and robust IT security are required to be implemented in order to safeguard the confidentiality and integrity of medical data.

Wearable IoMT devices facilitate the acquisition of real-time biometric data, seamlessly integrated with cloud applications and smartphones, thereby capturing the user's physiological parameters [9]. Such devices streamline early detection processes for patients, obviating the need for physical visits to healthcare facilities and thereby optimizing time efficiency. The IoMT wearable spectrum encompasses smart devices designed for on-body usage and vital/health monitors suitable for diverse environments, from homes and hospitals to communities, all equipped with real-time location capabilities [10]. However, the inherent processing speed constraints of IoMT devices can impede their efficacy in real-time data analytics and decision-making. It is imperative to devise an innovative strategy that can adeptly manage decision-making processes on IoT-enabled microprocessors, especially given their restricted computational prowess.

Historically, IoMT devices have served as conduits connecting physicians and patients within healthcare environments. A myriad of diagnostic tests, spanning ultrasounds, blood pressure evaluations, ECG, EEG, and glucose receptor assays, have been employed to vigilantly monitor patient health. The significance of subsequent medical consultations is underscored. Innovations like smart beds, prevalent in select medical facilities, possess the capability to discern patient movements, subsequently modulating bed orientation and elevation autonomously [11]. Sole reliance on a singular medical signal often falls short in ensuring precise disease diagnosis. In such scenarios, amalgamating multimodal medical signals emerges as a potent diagnostic enhancer [12]. Yet, the fusion of these signals introduces complexities, notably in synchronizing multi-sensor inputs, feature normalization, and classifier integration [13]. Traditional IoMT predominantly emphasizes data collation and its relay to centralized systems for comprehensive analysis and informed decision-making, often leveraging conventional algorithms and rule-centric analytical systems. The proliferation of Artificial Intelligence (AI) and advancements in wireless local area network (WLAN) technologies have catalyzed the evolution of intelligent healthcare, optimizing patient experiences and catering to the requisites of medical professionals [14]. Nonetheless, traditional AI methodologies grapple with the challenges posed by inherently error-prone data. Such data anomalies can be adeptly mitigated and refined through the deployment of Deep Learning (DL) [15] and EFL paradigms [16].

This study amalgamates recent research on emerging IoMT technologies to conduct a comprehensive review of the current literature. Additionally, it delves into the challenges that AI-powered IoMT may confront in the coming years. The following are the study's primary contributions:

- This study provides an overview of the conventional architecture of IoMT, which involves a centralized data

silo to collect streaming data from edge sensory nodes. We examine the fundamental IoT technologies used in the medical domain, highlight their limitations, and suggest research directions to enhance data accuracy and reduce errors. Furthermore, we analyze existing IoMT applications and describe a distinctive use case: wearable personal health monitoring systems.
- Considering the swift expansion of medical data and the intricate nature of data organization, this investigation focuses on the framework of cloud-edge computing for IoMT. This study explores the technologies used to apply cloud-edge AI to IoMT and emphasizes bringing AI inference engine closer to the user.
- By integrating EFL with IoMT, high-quality diagnostics can be achieved, thereby improving healthcare and enhancing patient outcomes. Utilizing EFL algorithms, IoMT devices equipped with sensors and data collection capabilities can continuously monitor patient health, analyze large amounts of data, detect early diseases, and personalize treatment plans. Finally, the future research direction involving AI-powered IoMT shows significant promise for advancing medical monitoring and treatment.

This paper explores the current trends in academic literatures concerning wearable health monitoring enabled by the IoMT and identifies several issues that need attention to make healthcare technologies more personalized for patients. The data collection method was carried out by searching online literature on medical matters at PUBMED, Science Direct, and the IEEE Library using the terms ('Internet of Medical Things', 'Medical Big Data', 'Cloud-edge Computing', and 'Artificial Intelligence of Things'). Context relevance (content related to IoMT in healthcare) and full-text availability were also considered.

The rest of this study is organized as follows: In Section II, this study introduces big medical data driven by IoMT-enabled personal health monitoring. Section III introduces a novel cloud-edge IoMT architecture that brings the compute unit and decision support systems closer to the medical institution and even to the patients. Section IV discusses the challenges and future directions of AI-driven IoMT devices for effective utilization of medical resources. Finally, Section V concludes this study.

II. BIG MEDICAL DATA DRIVEN BY IOMT

The use of IoMT technology in the medical field highlights the importance of organizing medical data, such as patient health records [17]. In conventional medical assessments, data was traditionally collected using paper-based methods. However, with modern approaches, patient records will increase rapidly due to the use of both conventional wearable monitors [18] and tattoo-based epidermal biosensors (i.e., e-tattoo) [19] producing real-time biomarker data continuously. The conventional wearable monitors would be impractical for extended durations, but e-tattoos enable attachment to body parts. The utilization of flexible and thin materials facilitates closer and more intimate contact with the user's skin than achievable with rigid sensors, a critical factor for accurately measuring the body's electrical impulses. This design results in a device that offers greater comfort compared to traditional wearables, and, in numerous instances, can collect data that was traditionally obtainable only within a controlled laboratory or hospital environment. Medical personnel can now focus more on patient-centered care instead of the extensive task of recording and organizing vast amounts of medical data. This shift enhances the quality of medical services provided. This section introduces the architecture of IoMT, IT infrastructures for centralized cloud data management, and optimizations related to security and privacy.

A. ARCHITECTURE OF IOMT

IoMT-enabled sensing devices have revolutionized healthcare. They integrate advanced technologies into various wearable personal health monitoring systems, offering continuous monitoring, early diagnosis, and remote therapy. Notable among these sensing devices are Implanted Cardioverter Defibrillators (ICDs) [20] and Wearable Cardioverter Defibrillators (WCDs) [21]. These provide life-saving interventions for individuals with heart rhythm abnormalities. Wearable devices like smart bands [22], smart gloves [23], and smartwatches [24] enable continuous health monitoring and tracking, promoting proactive healthcare management. Wearable spirometers [25] are crucial for individuals to monitor their lung function, especially those with respiratory conditions. ECG patches [26] offer a non-invasive way to record electrocardiogram data over extended periods, aiding in the diagnosis of cardiac irregularities. These patches could be developed as ultra-thin e-tattoos allowing measurements in all kinds of situations. Insulin pumps [27] and Continuous Glucose Monitors (CGMs) [28] have significantly improved the lives of diabetics by offering precise glucose control and reducing the need for frequent blood sugar checks. For pain management, TENS therapy devices [29] deliver targeted electrical stimulation to alleviate discomfort. Additionally, intraoral camera [30] enhance dental care, allowing dentists to capture high-quality images of oral health issues for accurate diagnosis and treatment planning. Overall, IoMT devices impact a wide range of healthcare areas, from cardiovascular health to chronic disease management, pain relief, and dental care, ultimately improving patient quality of life and healthcare efficiency.

The proposed architecture is designed to facilitate seamless connectivity and communication among wearable personal health monitoring systems, cloud-based data management systems, and healthcare professionals. It comprises multiple layers that work in tandem to collect, transmit, and analyze medical data. To address this need, a comprehensive architectural mechanism has been delineated across various layers, as illustrated in FIGURE 1. At the data acquisition layer, sensing devices, such as wearable personal health monitoring

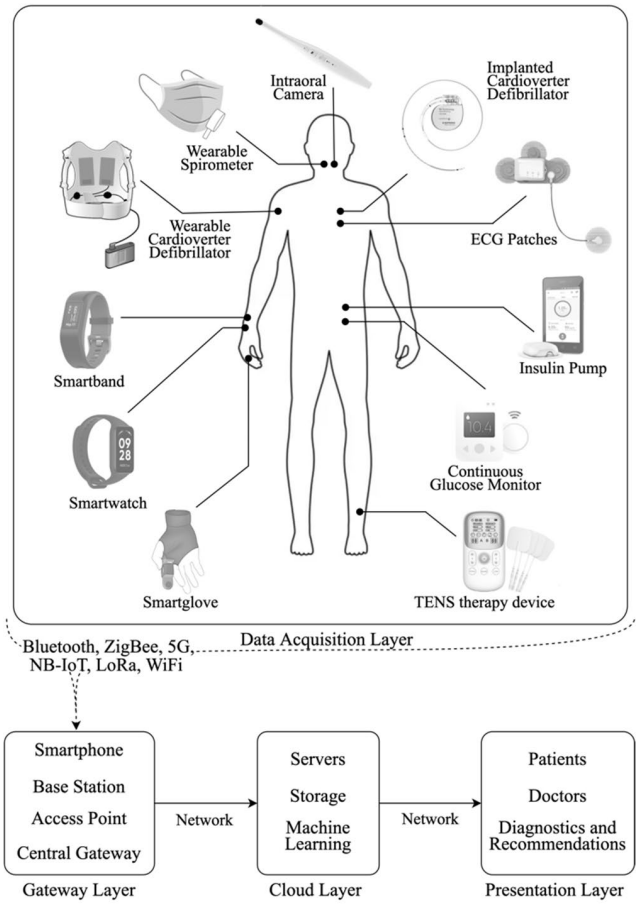

FIGURE 1. IoMT wearables utilize wireless connections to transmit real-time health data, thereby enhancing remote monitoring and patient care. In the IoMT architecture, a cloud-based data management system comprises multiple layers designed to deliver high-quality diagnostics to the patients.

systems, continuously capture patient data. This data is then securely transmitted to the gateway layer through wireless connection modules, including Bluetooth, ZigBee, 5G, NB-IoT, LoRa, and Wi-Fi. This layer incorporates stringent security measures, including secure communication protocols and robust authentication mechanisms, meticulously designed to prevent unauthorized access and ensure data integrity. The medical data is then sent to cloud computing platforms for further processing to develop generalized diagnostic models. Within the cloud layer, resilient servers provide computational resources for the storage, processing, and contextualization of medical data using advanced artificial intelligence techniques. Finally, the insights and results derived from the analysis are delivered to healthcare users and providers via websites or mobile applications. This architecture equips healthcare professionals with invaluable tools to deliver precise and continuous diagnostics and data-driven recommendations to patients, enhancing the quality of healthcare delivery.

A key advantage of the proposed IoMT architecture is its ability to integrate and interoperate with diverse healthcare systems and sensing devices. It's essential to standardize communication protocols and data formats to ensure seamless data exchange and compatibility between different IoMT components. By adopting these common standards, healthcare providers can integrate data from various sources, such as electronic health records, medical devices, and patient monitoring systems, into a unified platform. This integration allows for comprehensive analysis and decision-making [31]. Data integrity is a pivotal aspect of the IoMT architecture, especially when safeguarding sensitive medical information from potential errors. Moreover, interoperability creates a connected healthcare ecosystem. In this ecosystem, stakeholders, including patients, healthcare providers, and researchers, can access and share data. This sharing enhances patient outcomes, enables personalized medicine, and facilitates medical research [32].

B. IOMT ENABLING TECHNOLOGIES

1) WIRELESS COMMUNICATION

One of the pivotal technologies in the Internet of Medical Things (IoMT) is wireless communication. Technologies like Wi-Fi, Bluetooth, and Zigbee facilitate data transmission between medical devices and the healthcare infrastructure without physical connections [33]. These technologies offer flexibility, mobility, and ease of deployment, making them particularly suited for IoMT applications. For example, Bluetooth Low Energy (BLE) is a popular choice for wearable health monitoring devices, enabling continuous data collection and transmission to centralized systems [34]. In contrast, Wi-Fi is prevalent in hospital settings, connecting medical devices for real-time data monitoring and integration with Electronic Health Record (EHR) systems [35].

Another pivotal communication technology in IoMT is cellular communication. Cellular networks, including 3G, 4G, and emerging 5G, offer wide-area coverage and reliable connectivity for medical devices and healthcare infrastructures. This type of communication facilitates remote patient monitoring, telemedicine, and real-time data transmission across both urban and rural regions [36]. For instance, 4G LTE technology has been instrumental in connecting mobile medical devices, allowing for the continuous monitoring of patients beyond conventional healthcare environments [37]. With the evolution of 5G technology, IoMT applications stand to gain from increased data speeds, reduced latency, and enhanced network reliability, further amplifying the potential of remote healthcare services [38].

Other notable communication technologies gaining prominence in IoMT include Narrowband Internet of Things (NB-IoT) and Long-Range Wide-Area Network (LoRaWAN). NB-IoT is a Low-Power Wide-Area Network (LPWAN) technology specifically designed to connect a vast number of devices efficiently and securely [39]. It offers extended coverage, improved battery life, and dependable connectivity, making it ideal for IoMT applications [40]. Similarly, LoRa (Long Range) is an LPWAN technology that facilitates

long-distance communication with minimal power consumption [41]. It provides extensive coverage, especially beneficial for applications in remote or rural areas where cellular connectivity might be sparse. Integrating both NB-IoT and LoRa into the IoMT infrastructure ensures enhanced connectivity and seamless transmission of vital health data [42].

When evaluating Wi-Fi, NB-IoT, LoRa, and 5G technologies for IoT applications in the realm of the Medical Internet of Things (IoMT), there are trade-offs based on their distinct characteristics and use cases. Wi-Fi provides high data rates and is apt for local area wireless connectivity within a confined range. It shines in environments where high-speed internet access is essential for numerous devices in a limited space, such as homes, offices, and public areas [43]. However, the Wi-Fi coverage is typically restricted to a specific area, and its performance can diminish due to signal interference and congestion from a shared spectrum [44]. The 5G technology, conversely, delivers ultra-fast data rates, low latency, and vast capacity, catering to a broad spectrum of applications, from autonomous vehicles to remote surgery and expansive IoT deployments. It boasts improved network efficiency, augmented capacity, and superior support for numerous simultaneous connections [45]. Yet, rolling out 5G infrastructure demands substantial investments, and its coverage might initially be restricted. Both NB-IoT and LoRa are tailored for low-power, long-range IoT device communication [46]. They offer broad coverage, operate on licensed frequency bands, and have low power consumption, making them ideal for applications demanding prolonged battery life and expansive area coverage [47]. However, these long-range protocols have diminished data rates compared to Wi-Fi and 5G, making them optimal for transmitting minimal data and supporting low-bandwidth IoT applications. NB-IoT and LoRa are especially fitting for IoMT applications that emphasize battery longevity, extended range, and the capability to connect numerous devices [48]. In essence, the trade-offs among Wi-Fi, 5G, NB-IoT, and LoRa encompass factors like data rate, coverage, power usage, latency, and deployment expenses.

2) MICROPROCESSOR FOR REMOTE SENSORS

The incorporation of high-performance microprocessors into IoMT devices has been transformative for healthcare, paving the way for advanced data processing, analytics, and real-time decision-making at the edge. Microprocessors, such as those based on ARM architectures, deliver robust computing capabilities in compact form factors, making them perfectly suited for integration into medical devices and wearables. These microprocessors empower IoMT devices to amass and process vast amounts of data from diverse sensors, enabling instantaneous analysis and yielding actionable insights [49], [50], [51]. With the inclusion of microprocessors, IoMT devices can undertake functions like data filtering, signal processing, and the execution of artificial intelligence algorithms, equipping them to relay precise and timely data to healthcare practitioners and patients.

Incorporating microprocessors in IoMT devices significantly bolsters their connectivity and communication functionalities. Equipped with embedded Wi-Fi, Bluetooth, or cellular modules, these devices can effortlessly relay data to healthcare infrastructures, cloud platforms, or other interconnected devices [50], [51]. This facilitates remote surveillance, instantaneous data dissemination, and collaboration among medical professionals, thereby optimizing care coordination and enhancing patient outcomes. Furthermore, microprocessors within IoMT devices can champion edge computing, wherein data processing and analysis are executed directly on the device. This approach diminishes latency and bandwidth demands while fortifying data privacy and security measures [52], [53].

While the integration of microprocessors in IoMT devices brings a plethora of benefits, it also introduces certain challenges. Power consumption and energy efficiency stand out as paramount concerns, given that many IoMT devices rely on batteries and are expected to function over prolonged durations without regular recharging [50]. The safeguarding of sensitive patient data, processed by these microprocessors, is another critical aspect, necessitating stringent encryption, authentication, and access control measures [49]. Additionally, addressing the compatibility and standardization of microprocessor architectures and their associated software frameworks is essential. This ensures that diverse IoMT devices can achieve interoperability and integrate smoothly into pre-existing healthcare systems [50].

3) WEARABLE PERSONAL HEALTH MONITORING SYSTEMS

Wearable personal health monitoring systems, powered by IoMT devices, stand out as an innovative technology for the perpetual monitoring and oversight of individual health metrics. These systems amalgamate a variety of sensors and devices into wearable configurations, enabling non-intrusive and instantaneous tracking of vital signs, physical exertion, sleep cycles, and other pertinent health metrics. Such systems hold the promise of equipping individuals with the tools to proactively manage their health, paving the way for early health issue identification and tailored healthcare strategies. Furthermore, these wearable instruments bolster remote surveillance, granting healthcare practitioners access to precise and up-to-date patient information. This, in turn, augments the provision of distant healthcare services and better patient outcomes.

Numerous research endeavors have underscored the effectiveness and promise of wearable personal health monitoring systems. For example, in Ref. [54], the authors emphasized the significance of wearable instruments in gauging heart rate variability and its correlation with stress indicators. In Ref. [55], the authors delved into the utility of wearable sensors in pinpointing irregular gait patterns, offering early detection and intervention opportunities for Parkinson's

disease. In Ref. [56], the authors elaborated on the role of wearable devices in scrutinizing sleep cycles and their implications for holistic health and wellness. In Ref. [57], the authors probed into the adoption of wearable sensors for uninterrupted glucose surveillance in diabetic patients, yielding crucial insights for tailored diabetes care. Lastly, in Ref. [58], the authors examined the capacity of wearable tools in monitoring physical exertion and fostering a more active lifestyle.

These investigations cumulatively underscore an expanding corpus of evidence that attests to the efficacy and adaptability of wearable personal health monitoring systems. Bolstered by strides in sensor innovation, data analytics, and wireless connectivity, these systems are poised to redefine healthcare delivery, championing continuous surveillance, precocious detection of health anomalies, and tailored interventions [59]. However, there is an imperative need for further research to address prevailing challenges, including data privacy, data accuracy, user adoption, and the smooth integration of wearable devices into healthcare frameworks. Fundamentally, wearable personal health monitoring systems possess the capability to profoundly shape healthcare outcomes and inspire individuals to actively participate in their health management.

C. SECURITY AND PRIVACY ON CENTRALIZED MEDICAL DATA SILOS

Ensuring security and privacy stands as a foremost priority in the realm of centralized medical data repositories. Such healthcare repositories [60], [61] amass vast quantities of delicate patient data [62], encompassing personal health records, medical chronicles, and diagnostic evaluations. While the centralization paradigm proffers advantages like expedited data retrieval and cohesive healthcare workflows, it concurrently ushers in pronounced vulnerabilities [63]. Unauthorized access, data infringements, and malicious attacks jeopardize the sanctity and wholeness of patient information. The ramifications of these security lapses can be extensive, spanning from identity usurpation and deceit to undermining patient well-being and eroding confidence in healthcare infrastructures [64]. Hence, stringent security protocols, inclusive of encryption, access governance, and breach detection mechanisms, are imperative to shield the confidentiality of medical information within these centralized repositories.

Beyond security implications, privacy stands as an indispensable facet in the administration of centralized medical data repositories. Patients inherently anticipate their personal health records to be treated with paramount discretion and accessed solely when requisite. Yet, the consolidated framework of these data repositories amplifies apprehensions regarding potential data misappropriation or unwarranted dissemination [65]. Infringements of privacy can precipitate reputational tarnish, legal ramifications, and a diminution of patient confidence in medical institutions. To counteract these issues, rigorous privacy edicts and mandates, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), have been instituted to guarantee judicious management and processing of health data [66]. In tandem, methodologies like pseudonymization [67], anonymization [68], and consent orchestration systems [69] are pivotal in fortifying patient privacy, curtailing re-identification risks, and endowing individuals with amplified dominion over their data. In essence, harmonizing data security with privacy in centralized medical data repositories is imperative to sustain the faith of patients and medical stakeholders. Through the deployment of fortified security protocols and adherence to privacy statutes [70], medical entities can safeguard sensitive health data and curtail vulnerabilities linked to unauthorized intrusions and data infractions.

III. COMPUTING ARCHITECTURE FOR IOMT

Within a cloud computing paradigm, IoMT sensory nodes relay medical data from terminal devices to distant servers, subsequently reverting the processed outcomes back to the terminal apparatus. However, the burgeoning volume of data generated by the escalating array of medical instruments presents formidable challenges during its transmission to cloud platforms. Such a scenario exerts pronounced pressure on the cloud infrastructure, culminating in augmented energy expenditure and pronounced latencies owing to the overwhelming data influx. Sole dependence on cloud computing proves inadequate in managing such voluminous data streams and furnishing instantaneous feedback. Consequently, the evolution of medical cloud IoT hinges on proficiently amplifying the bandwidth of cloud computing and harnessing distributed computational assets. This strategy encompasses executing computational chores at the periphery of the network, as corroborated by studies [71], and the integration of edge computing emerges as an apt remedy to cater to these computational demands [72]. This segment elucidates the architecture of cloud-edge computing tailored for IoT, ensuring adept communication, efficacious processing, and the transformation of medical data into premium medical diagnostic insights.

A. CLOUD-BASED COMPUTING

Cloud-based computing has revolutionized the modus operandi of enterprises in addressing their computational requisites, proffering solutions that are both scalable and adaptable [73]. As delineated in a research article from the Journal of Information Technology, cloud computing has ascended as a prevailing framework within the information technology domain [74]. This paradigm empowers entities to harness computational resources and amenities via the internet, obviating the imperative for exorbitant in-house infrastructures. The inherent scalability of cloud computing capacitates organizations to modulate their resources in alignment with exigencies, guaranteeing pinnacle efficacy and

cost-effectiveness [75]. Moreover, this model has catalyzed the assimilation of avant-garde technologies like artificial intelligence and voluminous data analytics, given that these computation-intensive endeavors can be seamlessly relegated to the cloud [76].

Cloud-based computing proffers a plethora of advantages to enterprises, encompassing augmented collaboration and the facilitation of remote work capabilities [77]. An exposition in the Journal of Management Information Systems elucidated that tools anchored in cloud-based collaboration amplify team productivity and foster unbroken communication amongst team constituents [78]. Through the medium of cloud platforms, users can seamlessly access shared repositories, engage in real-time document collaboration, and utilize unified communication conduits. Such functionalities have garnered pronounced significance in the milieu of remote work, capacitating teams to synergize efficaciously irrespective of their geospatial coordinates. Furthermore, cloud computing equips organizations with the prowess to harness sophisticated analytics and data manipulation capabilities, thus catalyzing data-centric decision-making processes [79].

Albeit the myriad benefits proffered by cloud-based computing, apprehensions pertaining to security and privacy loom large. An erudite discourse in the Journal of Internet of Things underscored the imperativeness of navigating these quandaries [80]. To fortify the bulwark against potential breaches, cloud service purveyors have instituted a gamut of security stratagems, encompassing encryption, stringent access governance, and periodic security audits [81]. Notwithstanding these measures, it's incumbent upon organizations to meticulously implement their own protective mechanisms and assiduously assess the security protocols and accreditations proffered by cloud vendors. The academic fraternity has also ventured into pioneering modalities to augment security within the cloud ambit, delving into realms like secure data dissemination and techniques that prioritize privacy preservation [82]. As illustrated in FIGURE 2, IoMT devices, i.e., wearable personal health monitors, play a pivotal role in gathering and transmitting real-time medical data to the cloud for AI-enabled decision-making systems. The decision-making systems can be divided into two prominent approaches: the cloud-centric and edge-centric models. The fundamental difference between these approaches lies in the processing infrastructure. In the cloud-centric model, AI computational tasks are directed to centralized server infrastructures. In contrast, the edge-centric model promotes the use of compact AI models that are customized for direct execution on edge devices.

B. THE RISE OF EDGE COMPUTING

The advent of edge computing has significantly transformed the computing paradigm by shifting processing and analytical capabilities closer to the data source [83]. This shift towards decentralization has become indispensable given the surge in IoT devices and the ensuing demand for real-time processing coupled with low-latency responses. As underscored in a study featured in IEEE Cloud Computing, edge computing decentralizes computing tasks to the network's periphery [84]. Through the utilization of edge devices and gateways, edge computing not only accelerates data processing but also curtails network bandwidth consumption, bolstering both security and privacy [85].

Edge computing presents a myriad of benefits over conventional cloud computing paradigms [86]. One of its primary advantages is the substantial reduction in latency, as it circumvents the need to relay data to centralized cloud servers for processing. By facilitating local data processing, edge computing paves the way for instantaneous decision-making and expedited response times [87]. Moreover, by curtailing the volume of data transmitted to the cloud, edge computing alleviates network bandwidth pressures [88]. This becomes especially salient in contexts where prodigious amounts of data are generated, exemplified by industrial IoT deployments. An exhaustive survey featured in IEEE Access underscores the potential of edge computing in augmenting system performance and mitigating network congestion [89].

While edge computing boasts a plethora of merits, it is not devoid of challenges [90]. Its inherent distributed architecture engenders intricacies in the orchestration and management of edge devices and their corresponding applications. A paramount concern is the assurance of data security and privacy at the edge. The academic community is fervently delving into solutions to these quandaries, with a focus on fortified communication protocols and rigorous authentication frameworks [91]. An emergent paradigm, fog computing, which broadens the scope of edge computing to encompass a more expansive network architecture, is posited as a potential panacea to the constraints inherent to edge computing [92]. Through the adoption of fog computing, data processing can be disseminated across a nexus of edge devices, gateways, and centralized cloud infrastructures, fostering a more scalable and efficacious edge computing milieu. In summation, the ascendancy of edge computing heralds a transformative phase in computing, emphasizing proximate data processing [93]. It proffers advantages such as diminished latency, augmented real-time decision-making capabilities, and alleviated network congestion. Yet, to fully harness the potential of edge computing, pressing challenges in areas like management, security, and privacy necessitate meticulous attention and resolution [94].

C. CLOUD-EDGE AI ARCHITECTURE FOR IOMT

The Cloud-Edge AI architecture for the IoMT represents a vanguard paradigm that synergistically harnesses the prowess of both cloud and edge computing modalities to foster avant-garde healthcare applications [95]. As delineated in FIGURE 3, within the Cloud-Edge AI framework, the cloud epitomizes a centralized nexus dedicated to processing, archiving voluminous medical datasets, and facilitating intricate dataset training. Concurrently, edge entities are entrusted

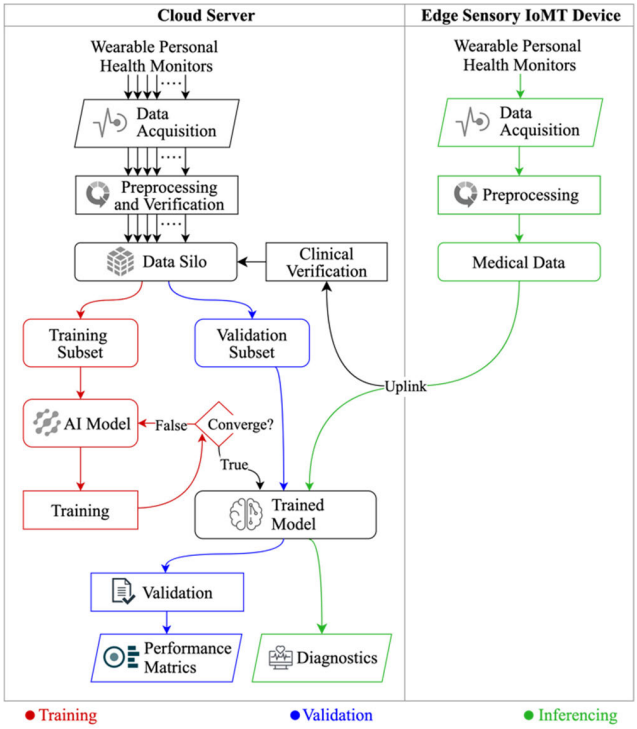

FIGURE 2. Within the IoMT domain, the prevailing AI architectural landscape is bifurcated into two salient paradigms: cloud-centric and edge-centric. The crux of the distinction between these paradigms is anchored in the locus of AI processing. Under the cloud-centric paradigm, AI computational tasks are relegated to centralized server infrastructures. Conversely, the edge-centric paradigm champions the deployment of svelte AI models, tailored for execution directly on edge devices.

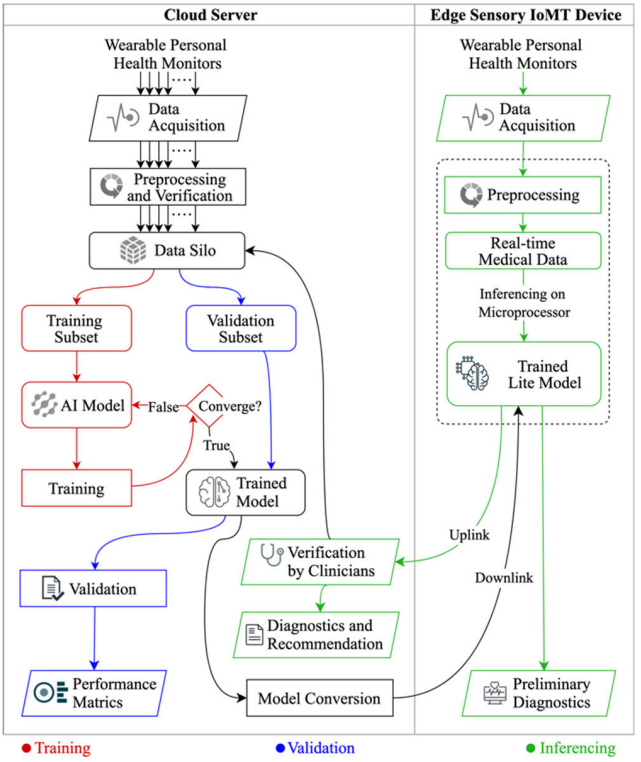

FIGURE 3. The envisaged cloud-edge AI architecture for IoMT is poised to usher in proximate clinical decision-support mechanisms to the medical user-provider nexus. Within the cloud-centric paradigm, data validation transpires in a centralized milieu, facilitating the dispensation of high-precision diagnostics anchored on rigorously curated datasets. In contrast, the edge-centric approach entails the transmutation of a server-originated trained model into a more compact representation. This streamlined model is subsequently instantiated on edge sensory apparatuses, thereby inaugurating an inference engine proximal to the data source. Such an arrangement amplifies the propensity for instantaneous data processing and elucidation, an indispensable attribute for IoMT endeavours.

with real-time data processing and inferencing at the network's periphery [96]. This bifurcated computational model bestows a multitude of advantages upon the IoMT milieu. It champions minimal-latency processing, attenuates network congestion, and guarantees prompt responses pivotal for exigent healthcare applications. The infusion of AI inferencing at the edge catalyzes sagacious decision-making, paving the way for real-time surveillance, diagnostic precision, and bespoke healthcare interventions. By capitalizing on the cloud's inherent scalability and adaptability, healthcare practitioners are empowered to adeptly curate and scrutinize copious medical data, culminating in enhanced patient welfare, precocious disease detection, and a more streamlined healthcare provision paradigm.

AI inferencing executed on microprocessors/microcontrollers encapsulates the actuation of pre-trained AI paradigms on resource-restricted microcontroller apparatuses [97]. Historically, AI undertakings necessitated the computational heft of robust servers or GPUs, given their intensive computational demands. Consequently, these servers proffered the computational prowess requisite for assimilating data from the edge, amalgamating it into a medical big data corpus, and subsequently orchestrating training protocols. Contrarily, edge microprocessors, due to their circumscribed computational capacity, were deemed unsuitable for intricate AI training procedures [98]. However, with the advent of hardware and software refinements, the deployment of AI inference engines directly onto microprocessors has become feasible, ushering in an era of intrinsic device acumen and edge computational proficiencies. For example, in Ref. [99], a non-invasive blood glucose monitor utilizing an ESP32 microprocessor and a photoplethysmography (PPG) MAX 30102 sensor to record pulse waves at the fingertips, was developed. In this study with 22 participants, non-invasive PPG data were classified into three classes by referencing conventional invasive measurements. A cloud-based AI training mechanism, specifically Convolutional Neural Networks (CNNs), was employed to align the proposed approach. The training mechanisms were still performed on cloud servers. Then, the trained model was converted into an AI Lite version that can be executed on a microprocessor locally. AI Lite models refer to streamlined and resource-efficient artificial intelligence models designed for deployment in environments with limited computational resources. AI inferencing at the edge via microprocessors proffers a plethora of merits. Primarily, it facilitates instantaneous decision-making, obviating

TABLE 1. Comparation between cloud computing, edge computing, and cloud-edge computing to support the development of IoMT concept.

Factors	Cloud Computing [73]	Edge Computing [83]	The Proposed Cloud-Edge Computing
Computing architecture	Centralized	Distributed	Centralized and distributed
Location	Cloud server	Edge nodes	Cloud server and edge nodes
Transmission bandwidth load	High	Low	Fair
Energy consumption	High	Low	Fair
Data processing	High	Low	Fair
Latency	High	Low	Low
Real time	Weak	Strong	Strong
Security	Low	High	Fair
Reliability	High	Low	Fair
Computing resources	Unlimited	Limited	Fair
Computing cost	High	Low	Fair
User experience	Weak	Strong	Strong

the dependency on cloud tethering, thereby expediting diagnostics and equipping medical professionals with the tools to dispense superior diagnostics and counsel. Furthermore, the instantiation of AI paradigms on microprocessors diminishes the imperative for incessant data relay, a boon in scenarios where bandwidth is either constrained or financially prohibitive. Additionally, localized inferencing on microprocessors curtails the latency inherent in data shuttling to the cloud, rendering it apt for applications demanding prompt and minimal-latency processing, such as robotic integrations and surgical automations.

TABLE 1 presents a comparison between cloud, edge, and cloud-edge computing, highlighting that cloud-edge computing is an extension of both cloud computing and edge computing concepts. Edge computing and cloud computing have a collaborative and complementary relationship. While edge devices can quickly analyze and process real-time data, most of the data is not used only once. Even after recording at the edge, data still needs to be transmitted from the edge devices to the cloud [100]. Tasks such as mining and analyzing massive data, storing crucial information, and linking multiple edge nodes heavily rely on the cloud. Additionally, the virtualization resources and management of edge devices also require cloud involvement. On the other hand, cloud-edge computing provides low latency, real-time data analytics, and a strong user experience [101]. In the development of AI applications, cloud-edge scenarios are feasible to be developed by focusing the server to train dan to validate datasets that are steamed continuously by the edge sensory nodes. Meanwhile, edge sensory nodes also provide AI-capable computational resources to infer real-time data generating early diagnostics for the patients. By closely implementing cloud-edge computing, they can cater to diverse demand scenarios, thus maximizing the application potential of cloud-edge technologies [102].

IV. RESEARCH CHALLENGES AND FUTURE FOR AI-POWERED IOMT

The incorporation of artificial intelligence (AI) across various healthcare domains, including diabetes management [103], clinical decision support frameworks [104], and robot-assisted surgeries [105], has been elucidated in extant literature. AI emerges as a linchpin in adeptly managing the voluminous and multifaceted sensor-generated data, thereby enabling granular analyses and bolstering decision-making prowess. This segment delineates the superiorities of AI-augmented IoMT vis-à-vis its conventional counterpart and prognosticates the trajectory of future advancements.

A. COMBINING WEARABLE IOMT DEVICES WITH 6G NETWORKS

The advent of 6G communication technologies is poised to usher in a plethora of innovations and opportunities within the IoT landscape [106]. Concurrently, it introduces a myriad of intricacies that necessitate meticulous attention to ensure the seamless amalgamation of 6G and IoT paradigms. A salient challenge lies in the exponential surge in data magnitude and intricacy. Given the prodigious speed and minuscule latency intrinsic to 6G, IoT apparatuses are anticipated to engender data at an unparalleled scale [107]. To adeptly manage, process, and interpret this data contemporaneously, there's an imperative for state-of-the-art computing architectures, efficacious data storage modalities, and sophisticated data analytics methodologies.

An additional challenge pertains to the security and privacy of IoT devices and the data they generate. With the anticipated exponential proliferation of connected devices, fortifying the security framework of IoT networks becomes paramount. It is imperative for 6G networks to embed rigorous security measures, encompassing end-to-end encryption, stringent authentication protocols, and sophisticated intrusion detection mechanisms, to shield sensitive IoT data and thwart potential cyber-attacks [108]. Furthermore, the issues of interoperability and standardization loom large in the nexus of 6G and IoT [109]. Given the heterogeneity of the IoT landscape, characterized by an array of devices and platforms from myriad manufacturers, each operating on distinct protocols and communication standards, forging seamless interoperability and achieving comprehensive standardization are indispensable. Such harmonization is pivotal to facilitate fluid communication, efficacious data interchange, and synergistic collaboration amongst diverse IoT systems.

Furthermore, the imperative of energy efficiency for IoT devices operating within 6G networks cannot be understated. Given that a significant proportion of IoT devices are reliant on battery power, and in light of the anticipated surge in the number of such connected entities, energy consumption emerges as a salient concern [110]. The onus is on innovators to engineer energy-frugal IoT devices, refine communication protocols for optimal energy utilization, and delve

into alternative energy reservoirs. Such endeavors aim to extend the operational longevity of IoT devices and guarantee their sustainable functionality within the ambit of 6G networks [111]. Beyond the technical challenges, the discourse must also encompass the ethical and societal ramifications of 6G-integrated IoT paradigms. As the ubiquity of IoT intensifies, it engenders debates surrounding privacy, the sanctity of data ownership, and the principled utilization of data harvested by IoT [112]. It becomes incumbent upon stakeholders to architect holistic frameworks and promulgate regulations that judiciously address these ethical quandaries, all while nurturing innovation and amplifying the dividends of 6G and IoT [113]. By preemptively confronting these challenges, the amalgamation of 6G and IoT stands poised to catalyze transformative shifts across sectors, enriching our quotidian experiences with a more astute, interconnected, and fortified IoT landscape [114].

B. OPTIMIZATIONS OF AI TECHNIQUES

The ascendancy of edge computing paradigms is inextricably linked to the strides made in the domain of AI. Seminal to this evolution is the incorporation of AI chips into edge apparatuses, which acts as the linchpin for engendering astute computations at the network periphery [115]. This symbiosis of AI algorithms and edge computing augments the velocity, security, and efficacy of data processing. Concurrently, it fine-tunes the apportionment of edge resources, thereby attenuating associated service expenditures. Presently, the epicentre of AI research gravitates towards DL, with concerted efforts directed at refining algorithms to surmount impediments such as non-convex optimization conundrums, the gradient dissipation phenomenon, and model overfitting. Owing to the intricate nature of objective functions inherent to DL, a plethora of optimization quandaries are bereft of analytical resolutions [116]. In such instances, recourse is often sought in approximation techniques, realized through optimization stratagems rooted in numerical methodologies, exemplified by stochastic gradient descent. Yet, formidable challenges persist, notably navigating the pitfalls of local optima in constrained dimensional spaces and contending with saddle points in expansive dimensional realms [117]. The relentless pursuit of algorithmic refinement is imperative to harness the full potential of edge apparatuses, thereby facilitating superior service delivery across a spectrum of medical application vistas.

1) EDGE AI

DL, a subfield of artificial intelligence, has burgeoned into a preeminent methodology, catalyzing transformative breakthroughs across multifarious sectors. Specifically, architectures such as spatiotemporal CNNs have been instrumental in redefining the AI landscape, facilitating intricate pattern discernment, adept natural language processing, and prescient analytics, albeit at the expense of intensive computational demands. Notwithstanding its prowess, the conventional

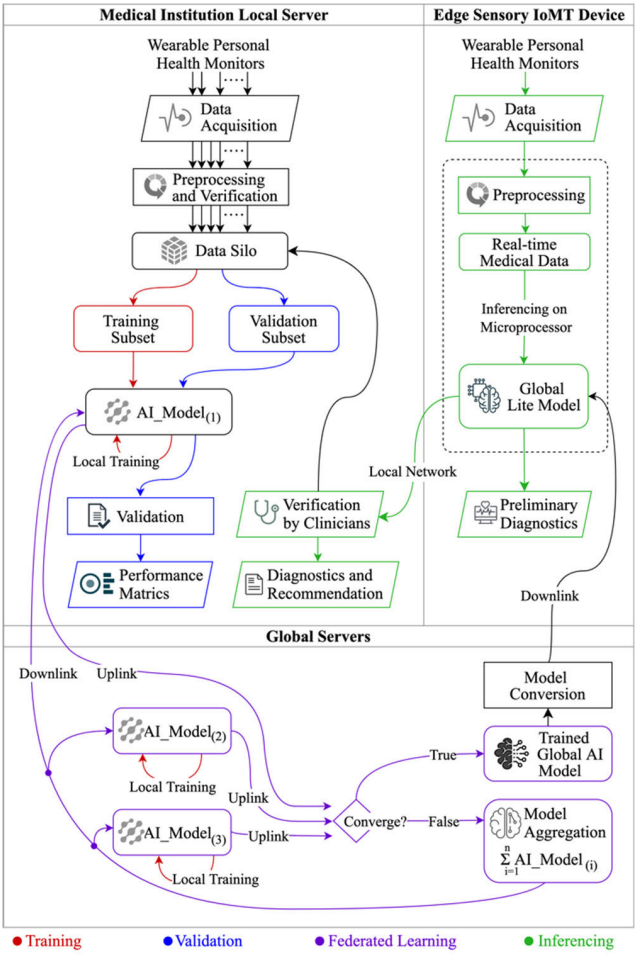

FIGURE 4. The envisaged cloud-edge federated AI architecture for IoMT presents a fortified clinical decision support mechanism, adeptly facilitating the exchange of medical data across institutions whilst circumventing the exposure of sensitive information to the broader cyberspace. In a bid to augment the efficacy of the prediction system, data emanating from IoMT devices is meticulously aggregated within each medical institution via a secure local network, thereby enriching the overarching dataset. In the subsequent phase, datasets collated from diverse medical institutions are subjected to Federated Learning protocols. This iterative methodology is operationalized leveraging a conventional internet connection, persisting until discernible patterns embedded within the datasets are adeptly generalized.

cloud-centric DL paradigm grapples with impediments in contexts characterized by circumscribed network bandwidth, exacting latency stipulations, and overarching privacy apprehensions. The advent of Edge AI, epitomized by the assimilation of DL blueprints directly onto edge apparatuses [118], offers a salient solution, orchestrating computations proximal to the data genesis locus. Harnessing the potential of edge computational faculties, DL schematics can be instantiated on edge devices with inherent resource constraints, engendering real-time inferencing and sagacious decision-making at the network periphery. This modus operandi not only diminishes dependency on nebulous cloud assets but also bolsters data confidentiality and fortification. Additionally, Edge AI paves the way for offline inferencing [119], equipping edge

contrivances with the capability to operate seamlessly, independent of a robust network linkage.

To facilitate DL inferencing on edge microprocessors, a plethora of optimization stratagems have been devised. These methodologies predominantly concentrate on model compression, quantization, and the formulation of neural network architectures meticulously tailored for microcontroller ecosystems [120]. Model compression paradigms endeavor to truncate the dimensions of the DL blueprint, rendering it compatible with the circumscribed memory reservoirs of microcontrollers. Concurrently, quantization approaches finetune the precision of weights and activations to curtail computational exigencies. Additionally, bespoke neural network architectures, such as svelte convolutional neural networks (CNNs) or spiking neural networks (SNNs), are architected to optimize efficacy whilst adhering to the resource stipulations of microcontrollers [121]. The confluence of DL and edge computing has catalyzed innovations across multifarious domains [122], encompassing autonomous robotics and perspicacious video surveillance. AI frameworks have emerged as pivotal tools to expedite the proliferation of AI at the edge.

TensorFlow Lite, a renowned AI framework, has been instrumental in facilitating the deployment of AI on edge devices [123]. The modus operandi for leveraging TensorFlow Lite entails the transformation of trained TensorFlow models into a compacted and optimized schema, primed for edge deployment. This streamlined iteration of TensorFlow ensures adept execution of AI paradigms on edge devices, which are often encumbered by limited computational prowess and memory constraints. Notably, TensorFlow Lite is compatible with an extensive array of hardware accelerators, thus ensuring its facile integration across a diverse spectrum of edge devices. By harnessing the capabilities of TensorFlow Lite, developers can actualize the potential of AI at the edge, engendering real-time and offline inference, bolstered data privacy and security, diminished latency, and an augmented user experience in their applications.

Another instrumental framework for orchestrating DL at the edge is PyTorch Mobile. Representing a refined iteration of the renowned PyTorch DL paradigm, PyTorch Mobile is meticulously crafted to facilitate the deployment of models on mobile and edge-centric devices [124]. This framework empowers developers to seamlessly transmute PyTorch models into configurations amenable to mobile environments, ensuring their operability on devices with constrained resources. PyTorch Mobile stands out by ensuring efficient and optimized execution for inference undertakings, endorsing salient features such as quantization, model fine-tuning, and hardware acceleration. Furthermore, its adaptability is underscored by its compatibility with diverse platforms, including Android and iOS. By harnessing PyTorch Mobile, developers can tap into the robust capabilities of PyTorch, capitalizing on its expansive ecosystem and user-friendly interface for on-device AI endeavors.

2) EDGE FEDERATED LEARNING

EFL has crystallized as a vanguard methodology, synergizing the merits of edge computing and federated learning to orchestrate collaborative and privacy-centric AI on edge devices. Within the EFL paradigm, raw data transmission to a monolithic server is eschewed. Instead, edge devices collaboratively refine a shared AI model, all the while retaining their data in a localized environment [125]. This decentralized learning framework fortifies data privacy and security, ensuring that sensitive datasets remain ensconced within the edge devices. EFL capitalizes on the computational prowess of edge devices, orchestrating local model refinements predicated on their distinct datasets. Notably, only the model's iterative updates are relayed to a central server [126]. This collaborative learning modality facilitates the model's refinement across a heterogeneous array of data sources, all the while adhering to stringent data privacy stipulations. The EFL paradigm, as delineated within the cloud-edge federated AI architecture, proffers a plethora of advantages over its traditional centralized AI counterparts (as illustrated in FIGURE 4. Foremost, it curtails the imperative for voluminous data transfers, thereby attenuating communication overheads and conserving bandwidth. Furthermore, by fostering local model training, this architecture catalyzes real-time inferencing and decision-making at the edge, obviating the need for persistent cloud connectivity. This attribute is particularly salient in scenarios where paramount importance is placed on low latency and offline functionalities, such as in IoT apparatus or sophisticated edge robotics. In summation, EFL augments the scalability quotient of AI systems, distributing computational burdens across a myriad of edge devices, thereby enhancing operational efficiency and diminishing reliance on centralized computational assets.

The modus operandi of federated learning, when contextualized within the ambit of the IoMT, encompasses a series of pivotal stages. The initial phase necessitates the orchestration of a cohesive network comprising medical apparatuses and sensors, tasked with the acquisition of data from a diverse array of sources, including but not limited to wearable health monitors, intricate medical implants, and dedicated health surveillance systems. Notably, this amassed data is retained in a decentralized fashion, ensconced within the confines of the originating devices or proximate edge servers, thereby fortifying its privacy and security attributes. Subsequent to this, the architecture of a federated learning paradigm is sculpted, wherein a central orchestrator or server choreographs the learning trajectory, albeit without direct ingress to the sensitive data reservoirs. In lieu of direct data access, this central entity disseminates model iterations or algorithmic updates to the localized devices or edge servers. These peripheral entities, leveraging their localized data caches, undertake the model training regimen and reciprocate by transmitting the refined parameters back to the central nexus. This cyclical process perpetuates, fostering a collaborative

learning milieu, all the while staunchly preserving data confidentiality. To bolster this privacy-centric stance, an array of sophisticated techniques, such as differential privacy and advanced encryption methodologies, can be seamlessly integrated. In its entirety, the federated learning blueprint within the IoMT framework champions a collaborative learning ethos derived from geographically dispersed data nodes, all the while tenaciously upholding data privacy and security tenets. Such an approach is poised to catalyze monumental strides in the realms of bespoke healthcare delivery and avant-garde medical research.

V. CONCLUSION

This research undertakes a comprehensive exploration of several IoMT paradigms, including centralized IoMT, cloud-edge-based IoMT, and AI-enhanced wearable IoMT, with a primary emphasis on medical data analytics and the evolution of clinical decision support mechanisms. In particular, the investigation delineates the architectural nuances of conventional IoMT and the associated IT infrastructure tailored for data management within centralized cloud environments. Furthermore, it underscores pivotal strategies aimed at bolstering data security and privacy. To address the inherent challenges associated with the traditional IoMT framework, this research introduces a novel cloud-edge AI blueprint, offering transformative solutions. Additionally, the research elucidates the manifold advantages proffered by EFL in amplifying the scalability of IoMT and offers insights into prospective trajectories in this domain. The Cloud-Edge AI architectural paradigm, tailored for the IoMT, emerges as an avant-garde approach, adeptly harnessing the synergies of cloud and edge computing to catalyze groundbreaking advancements in healthcare applications. As the IoMT ecosystem undergoes relentless evolution, synergistically intertwined with AI, the healthcare sector is poised to transition towards more proactive and preventive paradigms, rendering healthcare interventions increasingly patient-centric and bespoke.

REFERENCES

[1] A. Elliott, *The Culture of AI: Everyday Life and the Digital Revolution*. Evanston, IL, USA: Routledge, 2019.
[2] B. B. Bajgain, K. T. Bajgain, S. Badal, F. Aghajafari, J. Jackson, and M.-J. Santana, "Patient-reported experiences in accessing primary healthcare among immigrant population in canada: A rapid literature review," *Int. J. Environ. Res. Public Health*, vol. 17, no. 23, p. 8724, Nov. 2020.
[3] S. J. Shackelford, *The Internet of Things: What Everyone Needs To Know*. London, U.K.: Oxford Univ. Press, 2020.
[4] H. Landaluce, L. Arjona, A. Perallos, F. Falcone, I. Angulo, and F. Muralter, "A review of IoT sensing applications and challenges using RFID and wireless sensor networks," *Sensors*, vol. 20, no. 9, p. 2495, Apr. 2020.
[5] S. C. Kishore, K. Samikannu, R. Atchudan, S. Perumal, T. N. J. I. Edison, M. Alagan, A. K. Sundramoorthy, and Y. R. Lee, "Smartphone-operated wireless chemical sensors: A review," *Chemosensors*, vol. 10, no. 2, p. 55, Jan. 2022.
[6] A. A. Mathew, A. Chandrasekhar, and S. Vivekanandan, "A review on real-time implantable and wearable health monitoring sensors based on triboelectric nanogenerator approach," *Nano Energy*, vol. 80, Feb. 2021, Art. no. 105566.
[7] K. Zhan, "RETRACTED: Sports and health big data system based on 5G network and Internet of Things system," *Microprocessors Microsyst.*, vol. 80, Feb. 2021, Art. no. 103363.
[8] L. Sun, X. Jiang, H. Ren, and Y. Guo, "Edge-cloud computing and artificial intelligence in Internet of Medical Things: Architecture, technology and application," *IEEE Access*, vol. 8, pp. 101079–101092, 2020.
[9] E. A. Adeniyi, R. O. Ogundokun, and J. B. Awotunde, "IoMT-based wearable body sensors network healthcare monitoring system," in *IoT in Healthcare and Ambient Assisted Living*. Singapore: Springer, 2021, pp. 103–121.
[10] C. Dilibal, B. L. Davis, and C. Chakraborty, "Generative design methodology for Internet of Medical Things (IoMT)-based wearable biomedical devices," in *Proc. 3rd Int. Congr. Human-Computer Interact., Optim. Robotic Appl. (HORA)*, Jun. 2021, pp. 1–4.
[11] V. Davoodnia, M. Slinowsky, and A. Etemad, "Deep multitask learning for pervasive BMI estimation and identity recognition in smart beds," *J. Ambient Intell. Humanized Comput.*, vol. 14, no. 5, pp. 5463–5477, May 2023.
[12] H. Hermessi, O. Mourali, and E. Zagrouba, "Multimodal medical image fusion review: Theoretical background and recent advances," *Signal Process.*, vol. 183, Jun. 2021, Art. no. 108036.
[13] Y. Qian, H. Tang, Y. Ran, and B. Li, "Target classification in unattended ground sensors with a two-stream convolutional network," *IEEE Sensors J.*, vol. 23, no. 4, pp. 3747–3755, Feb. 2023.
[14] F. Tramarin, A. K. Mok, and S. Han, "Real-time and reliable industrial control over wireless LANs: Algorithms, protocols, and future directions," *Proc. IEEE*, vol. 107, no. 6, pp. 1027–1052, Jun. 2019.
[15] X. Liu, H. Wang, and Z. Li, "An approach for deep learning in ECG classification tasks in the presence of noisy labels," in *Proc. 43rd Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Nov. 2021, pp. 369–372.
[16] Prayitno, C.-R. Shyu, K. T. Putra, H.-C. Chen, Y.-Y. Tsai, K. S. M. T. Hossain, W. Jiang, and Z.-Y. Shae, "A systematic review of federated learning in the healthcare area: From the perspective of data properties and applications," *Appl. Sci.*, vol. 11, no. 23, p. 11191, Nov. 2021.
[17] W. Meng, Y. Cai, L. T. Yang, and W.-Y. Chiu, "Hybrid emotion-aware monitoring system based on brainwaves for Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 16014–16022, Nov. 2021.
[18] S. M. Rajagopal, M. Supriya, and R. Buyya, "FedSDM: Federated learning based smart decision making module for ECG data in IoT integrated edge-fog-cloud computing environments," *Internet Things*, vol. 22, Jul. 2023, Art. no. 100784.
[19] K. D. Belcastro and O. Ergen, "Digitize the human body by backscattering based nano-tattoos: Battery-free sensing," *IEEE Electron Device Lett.*, vol. 44, no. 5, pp. 849–852, May 2023.
[20] T. Campi, S. Cruciani, F. Maradei, A. Montalto, F. Musumeci, and M. Feliziani, "EMI in a cardiac implantable electronic device (CIED) by the wireless powering of a left ventricular assist device (LVAD)," *IEEE Trans. Electromagn. Compat.*, vol. 63, no. 4, pp. 988–995, Aug. 2021.
[21] M. Alsamman, A. Prashad, R. Abdelmaseih, T. Khalid, and R. Prashad, "Update on wearable cardioverter defibrillator: A comprehensive review of literature," *Cardiol. Res.*, vol. 13, no. 4, pp. 185–189, Aug. 2022.
[22] D. Ekiz, Y. S. Can, Y. C. Dardagan, and C. Ersoy, "Is your smartband smart enough to know who you are: Continuous physiological authentication in the wild," 2019, *arXiv:1912.04760*.
[23] S. Ghate, L. Yu, K. Du, C. T. Lim, and J. C. Yeo, "Sensorized fabric glove as game controller for rehabilitation," in *Proc. IEEE SENSORS*, Oct. 2020, pp. 1–4.
[24] K. Ueafuea, C. Boonnag, T. Sudhawiyangkul, P. Leelaarporn, A. Gulistan, W. Chen, S. C. Mukhopadhyay, T. Wilaiprasitporn, and S. Piyayotai, "Potential applications of mobile and wearable devices for psychological support during the COVID-19 pandemic: A review," *IEEE Sensors J.*, vol. 21, no. 6, pp. 7162–7178, Mar. 2021.
[25] M. Annabestani, P. Esmaeili-Dokht, S. K. Nejad, and M. Fardmanesh, "NAFAS: Non-rigid air flow active sensor, a cost-effective, wearable, and ubiquitous respiratory bio-sensor," *IEEE Sensors J.*, vol. 21, no. 7, pp. 9530–9537, Apr. 2021.
[26] D. Lai, Y. Bu, Y. Su, X. Zhang, and C.-S. Ma, "Non-standardized patch-based ECG lead together with deep learning based algorithm for automatic screening of atrial fibrillation," *IEEE J. Biomed. Health Informat.*, vol. 24, no. 6, pp. 1569–1578, Jun. 2020.

[27] G. Zheng, W. Yang, C. Valli, R. Shankaran, H. Abbas, G. Zhang, G. Fang, J. Chaudhry, and L. Qiao, "Fingerprint access control for wireless insulin pump systems using cancelable Delaunay triangulations," *IEEE Access*, vol. 7, pp. 75629–75641, 2019.

[28] J. Malik, S. Kim, J. M. Seo, Y. M. Cho, and F. Bien, "Minimally invasive implant type electromagnetic biosensor for continuous glucose monitoring system: In vivo evaluation," *IEEE Trans. Biomed. Eng.*, vol. 70, no. 3, pp. 1000–1011, Mar. 2023.

[29] A. F. Jadidi, W. Jensen, A. A. Zarei, and E. R. Lontis, "Alteration in cortical activity and perceived sensation following modulated TENS," *IEEE Trans. Neural Syst. Rehabil. Eng.*, vol. 31, pp. 875–883, 2023.

[30] M. A. Tily, H. Al-Nashash, and H. Mir, "An intraoral camera for supporting assistive devices," *IEEE Sensors J.*, vol. 21, no. 6, pp. 8553–8563, Mar. 2021.

[31] L. Rundo, R. Pirrone, S. Vitabile, E. Sala, and O. Gambino, "Recent advances of HCI in decision-making tasks for optimized clinical workflows and precision medicine," *J. Biomed. Informat.*, vol. 108, Aug. 2020, Art. no. 103479.

[32] L. Sharma, J. Olson, A. Guha, and L. McDougal, "How blockchain will transform the healthcare ecosystem," *Bus. Horizons*, vol. 64, no. 5, pp. 673–682, Sep. 2021.

[33] H. H. Alshammari, "The Internet of Things healthcare monitoring system based on MQTT protocol," *Alexandria Eng. J.*, vol. 69, pp. 275–287, Apr. 2023.

[34] T. Wu, F. Wu, C. Qiu, J.-M. Redouté, and M. R. Yuce, "A rigid-flex wearable health monitoring sensor patch for IoT-connected healthcare applications," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6932–6945, Aug. 2020.

[35] S. K. Jagatheesaperumal, P. Mishra, N. Moustafa, and R. Chauhan, "A holistic survey on the use of emerging technologies to provision secure healthcare solutions," *Comput. Electr. Eng.*, vol. 99, Apr. 2022, Art. no. 107691.

[36] M. Javaid, A. Haleem, R. P. Singh, and R. Suman, "5G technology for healthcare: Features, serviceable pillars, and applications," *Intell. Pharmacy*, vol. 1, no. 1, pp. 2–10, Jun. 2023.

[37] S. Sutradhar, S. Karforma, R. Bose, and S. Roy, "A dynamic step-wise tiny encryption algorithm with fruit fly optimization for quality of service improvement in healthcare," *Healthcare Analytics*, vol. 3, Nov. 2023, Art. no. 100177.

[38] Y. Liu and M. O. Al Kalaa, "Testing 5G user equipment: Review, challenges, and gaps from the medical device perspective," *IEEE Electromagn. Compat. Mag.*, vol. 11, no. 1, pp. 37–44, 1st Quart., 2022.

[39] F. Gu, J. Niu, L. Jiang, X. Liu, and M. Atiquzzaman, "Survey of the low power wide area network technologies," *J. Netw. Comput. Appl.*, vol. 149, Jan. 2020, Art. no. 102459.

[40] P. Sharma, S. Jain, S. Gupta, and V. Chamola, "Role of machine learning and deep learning in securing 5G-driven industrial IoT applications," *Ad Hoc Netw.*, vol. 123, Dec. 2021, Art. no. 102685.

[41] R. Marini, K. Mikhaylov, G. Pasolini, and C. Buratti, "Low-power wide-area networks: Comparison of LoRaWAN and NB-IoT performance," *IEEE Internet Things J.*, vol. 9, no. 21, pp. 21051–21063, Nov. 2022.

[42] B. Chaudhari and S. Borkar, "Design considerations and network architectures for low-power wide-area networks," in *LPWAN Technologies for IoT and M2M Applications*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 15–35.

[43] Md. M. Islam, S. Nooruddin, F. Karray, and G. Muhammad, "Internet of Things: Device capabilities, architectures, protocols, and smart applications in healthcare domain," *IEEE Internet Things J.*, vol. 10, no. 4, pp. 3611–3641, Feb. 2023.

[44] H. A. H. Alobaidy, M. J. Singh, M. Behjati, R. Nordin, and N. F. Abdullah, "Wireless transmissions, propagation and channel modelling for IoT technologies: Applications and challenges," *IEEE Access*, vol. 10, pp. 24095–24131, 2022.

[45] J.-P.-A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations," *Internet Things*, vol. 19, Aug. 2022, Art. no. 100544.

[46] X. Liu, K.-Y. Lam, F. Li, J. Zhao, L. Wang, and T. S. Durrani, "Spectrum sharing for 6G integrated satellite-terrestrial communication networks based on NOMA and CR," *IEEE Netw.*, vol. 35, no. 4, pp. 28–34, Jul. 2021.

[47] R. Akter, M. Golam, V.-S. Doan, J.-M. Lee, and D.-S. Kim, "IoMT-Net: Blockchain-integrated unauthorized UAV localization using lightweight convolution neural network for Internet of Military Things," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6634–6651, Apr. 2023.

[48] G. Leenders, G. Callebaut, G. Ottoy, L. van der Perre, and L. De Strycker, "Multi-RAT for IoT: The potential in combining LoRaWAN and NB-IoT," *IEEE Commun. Mag.*, vol. 59, no. 12, pp. 98–104, Dec. 2021.

[49] H. F. Ahmad, W. Rafique, R. U. Rasool, A. Alhumam, Z. Anwar, and J. Qadir, "Leveraging 6G, extended reality, and IoT big data analytics for healthcare: A review," *Comput. Sci. Rev.*, vol. 48, May 2023, Art. no. 100558.

[50] V. S. Naresh, S. S. Pericherla, P. S. R. Murty, and S. Reddi, "Internet of Things in healthcare: Architecture, applications, challenges, and solutions," *Comput. Syst. Sci. Eng.*, vol. 35, no. 6, pp. 411–421, 2020.

[51] M. N. Bhuiyan, M. M. Rahman, M. M. Billah, and D. Saha, "Internet of Things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10474–10498, Jul. 2021.

[52] N. Garg, M. S. Obaidat, M. Wazid, A. K. Das, and D. P. Singh, "SPCS-IoTEH: Secure privacy-preserving communication scheme for IoT-enabled e-Health applications," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2021, pp. 1–6.

[53] L. Zhang, Y. Zhu, W. Ren, Y. Zhang, and K.-K. R. Choo, "Privacy-preserving fast three-factor authentication and key agreement for IoT-based e-health systems," *IEEE Trans. Services Comput.*, vol. 16, no. 2, pp. 1324–1333, Mar./Apr. 2023.

[54] U. Pluntke, S. Gerke, A. Sridhar, J. Weiss, and B. Michel, "Evaluation and classification of physical and psychological stress in firefighters using heart rate variability," in *Proc. 41st Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Jul. 2019, pp. 2207–2212.

[55] H. Mughal, A. R. Javed, M. Rizwan, A. S. Almadhor, and N. Kryvinska, "Parkinson's disease management via wearable sensors: A systematic review," *IEEE Access*, vol. 10, pp. 35219–35237, 2022.

[56] M. Abouzahra and M. Ghasemaghaei, "The antecedents and results of seniors' use of activity tracking wearable devices," *Health Policy Technol.*, vol. 9, no. 2, pp. 213–217, Jun. 2020.

[57] A. M. Coates, J. N. Cohen, and J. F. Burr, "Investigating sensor location on the effectiveness of continuous glucose monitoring during exercise in a non-diabetic population," *Eur. J. Sport Sci.*, vol. 10, pp. 2109–2117, Oct. 2023.

[58] J. E. Caterini, E. S. Campisi, and B. Cifra, "Physical activity promotion in pediatric congenital heart disease: Are we running late?" *Can. J. Cardiol.*, vol. 36, no. 9, pp. 1406–1416, Sep. 2020.

[59] Y. Zhu et al., "Skin-interfaced electronics: A promising and intelligent paradigm for personalized healthcare," *Biomaterials*, vol. 296, May 2023, Art. no. 122075.

[60] S. Rachakonda, S. Moorthy, A. Jain, A. Bukharev, A. Bucur, F. Manni, T. M. Quiterio, L. Joosten, and N. I. Mendez, "Privacy enhancing and scalable federated learning to accelerate AI implementation in cross-silo and IoMT environments," *IEEE J. Biomed. Health Informat.*, vol. 27, no. 2, pp. 744–755, Feb. 2023.

[61] R. Ranchal, P. Bastide, X. Wang, A. Gkoulalas-Divanis, M. Mehra, S. Bakthavachalam, H. Lei, and A. Mohindra, "Disrupting healthcare silos: Addressing data volume, velocity and variety with a cloud-native healthcare data ingestion service," *IEEE J. Biomed. Health Informat.*, vol. 24, no. 11, pp. 3182–3188, Nov. 2020.

[62] R. Kumar, N. Marchang, and R. Tripathi, "Distributed off-chain storage of patient diagnostic reports in healthcare system using IPFS and blockchain," in *Proc. Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2020, pp. 1–5.

[63] M. Javaid, A. Haleem, R. P. Singh, and R. Suman, "Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends," *Cyber Secur. Appl.*, vol. 1, Dec. 2023, Art. no. 100016.

[64] F. Firouzi, B. Farahani, M. Barzegari, and M. Daneshmand, "AI-driven data monetization: The other face of data in IoT-based smart and connected health," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 5581–5599, Apr. 2022.

[65] K. Hui, C. J. Gilmore, and M. Khan, "Medical records: More than the health insurance portability and accountability act," *J. Acad. Nutrition Dietetics*, vol. 121, no. 4, pp. 770–772, Apr. 2021.

[66] M. Pedrosa, A. Zúquete, and C. Costa, "A pseudonymisation protocol with implicit and explicit consent routes for health records in federated ledgers," *IEEE J. Biomed. Health Informat.*, vol. 25, no. 6, pp. 2172–2183, Jun. 2021.
[67] S. Dimopoulou, C. Symvoulidis, K. Koutsoukos, A. Kiourtis, A. Mavrogiorgou, and D. Kyriazis, "Mobile anonymization and pseudonymization of structured health data for research," in *Proc. 7th Int. Conf. Mobile Secure Services (MobiSecServ)*, Feb. 2022, pp. 1–6.
[68] M. De Ree, D. Vizár, G. Mantas, J. Bastos, C. Kassapoglou-Faist, and J. Rodriguez, "A key management framework to secure IoMT-enabled healthcare systems," in *Proc. IEEE 26th Int. Workshop Comput. Aided Model. Design Commun. Links Netw. (CAMAD)*, Oct. 2021, pp. 1–6.
[69] F. Fotopoulos, V. Malamas, T. K. Dasaklis, P. Kotzanikolaou, and C. Douligeris, "A blockchain-enabled architecture for IoMT device authentication," in *Proc. IEEE Eurasia Conf. IoT, Commun. Eng. (ECICE)*, Oct. 2020, pp. 89–92.
[70] I. Lee, "Analyzing web descriptions of cybersecurity breaches in the healthcare provider sector: A content analytics research method," *Comput. Secur.*, vol. 129, Jun. 2023, Art. no. 103185.
[71] A. Islam, A. Debnath, M. Ghose, and S. Chakraborty, "A survey on task offloading in multi-access edge computing," *J. Syst. Archit.*, vol. 118, Sep. 2021, Art. no. 102225.
[72] M. Laroui, B. Nour, H. Moungla, M. A. Cherif, H. Afifi, and M. Guizani, "Edge and fog computing for IoT: A survey on current research activities & future directions," *Comput. Commun.*, vol. 180, pp. 210–231, Dec. 2021.
[73] F. Gao and A. Sunyaev, "Context matters: A review of the determinant factors in the decision to adopt cloud computing in healthcare," *Int. J. Inf. Manage.*, vol. 48, pp. 120–138, Oct. 2019.
[74] B. H. Banimfreg, "A comprehensive review and conceptual framework for cloud computing adoption in bioinformatics," *Healthcare Analytics*, vol. 3, Nov. 2023, Art. no. 100190.
[75] Z. Chang, S. Liu, X. Xiong, Z. Cai, and G. Tu, "A survey of recent advances in edge-computing-powered artificial intelligence of things," *IEEE Internet Things J.*, vol. 8, no. 18, pp. 13849–13875, Sep. 2021.
[76] M. Javaid, A. Haleem, R. P. Singh, S. Rab, R. Suman, and I. H. Khan, "Evolutionary trends in progressive cloud computing based healthcare: Ideas, enablers, and barriers," *Int. J. Cognit. Comput. Eng.*, vol. 3, pp. 124–135, Jun. 2022.
[77] S. A. Bello, L. O. Oyedele, O. O. Akinade, M. Bilal, J. M. D. Delgado, L. A. Akanbi, A. O. Ajayi, and H. A. Owolabi, "Cloud computing in construction industry: Use cases, benefits and challenges," *Autom. Construct.*, vol. 122, Feb. 2021, Art. no. 103441.
[78] S. Tarikere, I. Donner, and D. Woods, "Diagnosing a healthcare cybersecurity crisis: The impact of IoMT advancements and 5G," *Bus. Horizons*, vol. 64, no. 6, pp. 799–807, Nov. 2021.
[79] C. V. Anikwe, H. F. Nweke, A. C. Ikegwu, C. A. Egwuonwu, F. U. Onu, U. R. Alo, and Y. W. Teh, "Mobile and wearable sensors for data-driven health monitoring system: State-of-the-art and future prospect," *Expert Syst. Appl.*, vol. 202, Sep. 2022, Art. no. 117362.
[80] Y. Qiu, H. Zhang, and K. Long, "Computation offloading and wireless resource management for healthcare monitoring in fog-computing-based Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15875–15883, Nov. 2021.
[81] A. H. Mayer, V. F. Rodrigues, C. A. D. Costa, R. D. R. Righi, A. Roehrs, and R. S. Antunes, "FogChain: A fog computing architecture integrating blockchain and Internet of Things for personal health records," *IEEE Access*, vol. 9, pp. 122723–122737, 2021.
[82] A. Al Hadwer, M. Tavana, D. Gillis, and D. Rezania, "A systematic review of organizational factors impacting cloud-based technology adoption using technology-organization-environment framework," *Internet Things*, vol. 15, Sep. 2021, Art. no. 100407.
[83] F. M. Awaysheh, M. N. Aladwan, M. Alazab, S. Alawadi, J. C. Cabaleiro, and T. F. Pena, "Security by design for big data frameworks over cloud computing," *IEEE Trans. Eng. Manag.*, vol. 69, no. 6, pp. 3676–3693, Dec. 2022.
[84] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, "Security and privacy-preserving challenges of e-Health solutions in cloud computing," *IEEE Access*, vol. 7, pp. 74361–74382, 2019.
[85] Y. Mansouri and M. A. Babar, "A review of edge computing: Features and resource virtualization," *J. Parallel Distrib. Comput.*, vol. 150, pp. 155–183, Apr. 2021.
[86] B. Lin, F. Zhu, J. Zhang, J. Chen, X. Chen, N. N. Xiong, and J. L. Mauri, "A time-driven data placement strategy for a scientific workflow combining edge computing and cloud computing," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4254–4265, Jul. 2019.
[87] F. Al-Doghman, N. Moustafa, I. Khalil, N. Sohrabi, Z. Tari, and A. Y. Zomaya, "AI-enabled secure microservices in edge computing: Opportunities and challenges," *IEEE Trans. Services Comput.*, vol. 16, no. 2, pp. 1485–1504, Mar. 2023.
[88] L. Greco, G. Percannella, P. Ritrovato, F. Tortorella, and M. Vento, "Trends in IoT based solutions for health care: Moving AI to the edge," *Pattern Recognit. Lett.*, vol. 135, pp. 346–353, Jul. 2020.
[89] D. Liu, Z. Yan, W. Ding, and M. Atiquzzaman, "A survey on secure data analytics in edge computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4946–4967, Jun. 2019.
[90] K. H. Abdulkareem, M. A. Mohammed, S. S. Gunasekaran, M. N. Al-Mhiqani, A. A. Mutlag, S. A. Mostafa, N. S. Ali, and D. A. Ibrahim, "A review of fog computing and machine learning: Concepts, applications, challenges, and open issues," *IEEE Access*, vol. 7, pp. 153123–153140, 2019.
[91] D. C. Nguyen, M. Ding, Q.-V. Pham, P. N. Pathirana, L. B. Le, A. Seneviratne, J. Li, D. Niyato, and H. V. Poor, "Federated learning meets blockchain in edge computing: Opportunities and challenges," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12806–12825, Aug. 2021.
[92] P. Ranaweera, A. D. Jurcut, and M. Liyanage, "Survey on multi-access edge computing security and privacy," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 1078–1124, 2nd Quart., 2021.
[93] K. Baranitharan, V. Dineshbabu, R. Concepción-Lázaro, R. Balamanigandan, K. Selvakumarasamy, R. Mahaveerakannan, and M. W. Bhatt, "A collaborative and adaptive cyber défense strategic assessment for healthcare networks using edge computing," *Healthcare Analytics*, vol. 3, Nov. 2023, Art. no. 100184.
[94] R. Xie, Q. Tang, S. Qiao, H. Zhu, F. R. Yu, and T. Huang, "When serverless computing meets edge computing: Architecture, challenges, and open issues," *IEEE Wireless Commun.*, vol. 28, no. 5, pp. 126–133, Oct. 2021.
[95] S. Bebortta, S. S. Tripathy, S. Basheer, and C. L. Chowdhary, "DeepMist: Toward deep learning assisted mist computing framework for managing healthcare big data," *IEEE Access*, vol. 11, pp. 42485–42496, 2023.
[96] G. Rong, Y. Xu, X. Tong, and H. Fan, "An edge-cloud collaborative computing platform for building AIoT applications efficiently," *J. Cloud Comput.*, vol. 10, no. 1, pp. 1–14, Dec. 2021.
[97] Md. M. H. Shuvo, S. K. Islam, J. Cheng, and B. I. Morshed, "Efficient acceleration of deep learning inference on resource-constrained edge devices: A review," *Proc. IEEE*, vol. 111, no. 1, pp. 42–91, Jan. 2023.
[98] C. Mwase, Y. Jin, T. Westerlund, H. Tenhunen, and Z. Zou, "Communication-efficient distributed AI strategies for the IoT edge," *Future Gener. Comput. Syst.*, vol. 131, pp. 292–308, Jun. 2022.
[99] K. T. Putra, I. Surahmat, A. N. N. Chamim, M. Z. Ramadhan, D. Wicaksana, and R. A. Dhea Namyra Alissa, "Continuous glucose monitoring: A non-invasive approach for improved daily healthcare," in *Proc. 3rd Int. Conf. Electron. Electr. Eng. Intell. Syst. (ICE3IS)*, Yogyakarta, Indonesia, Aug. 2023, pp. 395–400.
[100] F. Firouzi, B. Farahani, and A. Marinšek, "The convergence and interplay of edge, fog, and cloud in the AI-driven Internet of Things (IoT)," *Inf. Syst.*, vol. 107, Jul. 2022, Art. no. 101840.
[101] Y. Sun, "Cloud edge computing for socialization robot based on intelligent data envelopment," *Comput. Electr. Eng.*, vol. 92, Jun. 2021, Art. no. 107136.
[102] X. Wang, Y. Han, V. C. M. Leung, D. Niyato, X. Yan, and X. Chen, "Convergence of edge computing and deep learning: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 869–904, 2nd Quart., 2020.
[103] K. Y. Ngiam and I. W. Khor, "Big data and machine learning algorithms for health-care delivery," *Lancet Oncol.*, vol. 20, no. 5, pp. e262–e273, May 2019.
[104] A. Haleem, M. Javaid, and I. H. Khan, "Current status and applications of artificial intelligence (AI) in medical field: An overview," *Current Med. Res. Pract.*, vol. 9, no. 6, pp. 231–237, Nov. 2019.
[105] A. Banerjee, C. Chakraborty, and M. Rathi, "Medical imaging, artificial intelligence, Internet of Things, wearable devices in terahertz healthcare technologies," in *Terahertz Biomedical and Healthcare Technologies*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 145–165.

[106] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, D. Niyato, O. Dobre, and H. V. Poor, "6G Internet of Things: A comprehensive survey," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 359–383, Jan. 2022.
[107] R. Ali, I. Ashraf, A. K. Bashir, and Y. B. Zikria, "Reinforcement-learning-enabled massive Internet of Things for 6G wireless communications," *IEEE Commun. Standards Mag.*, vol. 5, no. 2, pp. 126–131, Jun. 2021.
[108] H. J. Hadi, Y. Cao, K. U. Nisa, A. M. Jamil, and Q. Ni, "A comprehensive survey on security, privacy issues and emerging defence technologies for UAVs," *J. Netw. Comput. Appl.*, vol. 213, Apr. 2023, Art. no. 103607.
[109] M. Šarac, N. Pavlović, N. Bacanin, F. Al-Turjman, and S. Adamović, "Increasing privacy and security by integrating a blockchain secure interface into an IoT device security gateway architecture," *Energy Rep.*, vol. 7, pp. 8075–8082, Nov. 2021.
[110] A. Jahid, M. H. Alsharif, and T. J. Hall, "The convergence of blockchain, IoT and 6G: Potential, opportunities, challenges and research roadmap," *J. Netw. Comput. Appl.*, vol. 217, Aug. 2023, Art. no. 103677.
[111] Z. Lv, R. Lou, J. Li, A. K. Singh, and H. Song, "Big data analytics for 6G-enabled massive Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5350–5359, Apr. 2021.
[112] U. M. Malik, M. A. Javed, S. Zeadally, and S. U. Islam, "Energy-efficient fog computing for 6G-enabled massive IoT: Recent trends and future opportunities," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14572–14594, Aug. 2022.
[113] M. Uddin, S. Manickam, H. Ullah, M. Obaidat, and A. Dandoush, "Unveiling the metaverse: Exploring emerging trends, multifaceted perspectives, and future challenges," *IEEE Access*, vol. 11, pp. 87087–87103, 2023.
[114] K. R. Dhinesh and S. Chavhan, "Shift to 6G: Exploration on trends, vision, requirements, technologies, research, and standardization efforts," *Sustain. Energy Technol. Assessments*, vol. 54, Dec. 2022, Art. no. 102666.
[115] L. Cao, "Decentralized AI: Edge intelligence and smart blockchain, metaverse, Web3, and DeSci," *IEEE Intell. Syst.*, vol. 37, no. 3, pp. 6–19, May 2022.
[116] F. Hussain, S. A. Hassan, R. Hussain, and E. Hossain, "Machine learning for resource management in cellular and IoT networks: Potentials, current solutions, and open challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1251–1275, 2nd Quart., 2020.
[117] F.-L. Fan, J. Xiong, M. Li, and G. Wang, "On interpretability of artificial neural networks: A survey," *IEEE Trans. Radiat. Plasma Med. Sci.*, vol. 5, no. 6, pp. 741–760, Nov. 2021.
[118] E. Li, L. Zeng, Z. Zhou, and X. Chen, "Edge AI: On-demand accelerating deep neural network inference via edge computing," *IEEE Trans. Wireless Commun.*, vol. 19, no. 1, pp. 447–457, Jan. 2020.
[119] M. Xu, W. C. Ng, W. Y. B. Lim, J. Kang, Z. Xiong, D. Niyato, Q. Yang, X. Shen, and C. Miao, "A full dive into realizing the edge-enabled metaverse: Visions, enabling technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 656–700, 1st Quart., 2023.
[120] K. S. Zaman, M. B. I. Reaz, S. H. M. Ali, A. A. A. Bakar, and M. E. H. Chowdhury, "Custom hardware architectures for deep learning on portable devices: A review," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 33, no. 11, pp. 6068–6088, Nov. 2022.
[121] Z. Li, E. Lemaire, N. Abderrahmane, S. Bilavarn, and B. Miramond, "Efficiency analysis of artificial vs. spiking neural networks on FPGAs," *J. Syst. Archit.*, vol. 133, Dec. 2022, Art. no. 102765.
[122] H. Elazhary, "Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions," *J. Netw. Comput. Appl.*, vol. 128, pp. 105–140, Feb. 2019.
[123] C. Luo, X. He, J. Zhan, L. Wang, W. Gao, and J. Dai, "Comparison and benchmarking of AI models and frameworks on mobile devices," 2020, *arXiv:2005.05085*.
[124] N. C. A. Sallang, M. T. Islam, M. S. Islam, and H. Arshad, "A CNN-based smart waste management system using TensorFlow lite and LoRa-GPS shield in Internet of Things environment," *IEEE Access*, vol. 9, pp. 153560–153574, 2021.
[125] S. S. Shinde, A. Bozorgchenani, D. Tarchi, and Q. Ni, "On the design of federated learning in latency and energy constrained computation offloading operations in vehicular edge computing systems," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 2041–2057, Feb. 2022.
[126] A. F. X. Glória and P. J. A. Sebastião, "Autonomous configuration of communication systems for IoT smart nodes supported by machine learning," *IEEE Access*, vol. 9, pp. 75021–75034, 2021.

KARISMA TRINANDA PUTRA (Member, IEEE) received the bachelor's degree from the Electronic Engineering Polytechnic Institute of Surabaya, in 2012, the master's degree from the Sepuluh Nopember Institute of Technology, in 2015, and the Ph.D. degree from Asia University, Taiwan, in January 2022. He is currently an Assistant Professor and the Head of the Department of Electrical Engineering, Faculty of Engineering, Universitas Muhammadiyah Yogyakarta, Indonesia. His current research interests include the development of deep learning techniques, image processing, sensor networks, compressed sensing, and the Internet of Medical Things, particularly computational biology and medical data analysis. He is working on topics, including deep network inference on PM2.5 propagation, explainable analysis of medical data using XAI, and deep learning on microcontrollers for clinical decision support systems.

AHMAD ZAKI ARRAYYAN received the B.Eng. degree from Universitas Muhammadiyah Yogyakarta, in March 2023. He is currently pursuing the master's degree with the Islamic University of Indonesia, with a focus on the concentration of smart systems based on the Internet of Things. He works as a Lecturer Assistant with Universitas Muhammadiyah Yogyakarta. His research interests include machine learning and deep learning.

NUR HAYATI (Member, IEEE) received the bachelor's degree in applied science (telecommunications engineering) from the Electronic Engineering Institute of Surabaya, in 2010, and the master's and Ph.D. degrees in computer engineering from Universitas Indonesia, in 2015 and 2022, respectively. She is currently an Assistant Professor with the Department of Electrical Engineering, Universitas Muhammadiyah Yogyakarta. Her research interests include embedded systems, computer networks, and security in the IoT.

FIRDAUS (Member, IEEE) received the B.Eng. degree in electrical engineering from Gadjah Mada University, Yogyakarta, in 2007, the M.Eng. degree in telecommunication from Telkom University, Bandung, in 2010, and the Ph.D. degree from the Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Kuala Lumpur, in 2019. Currently, he is the Head of the Department of Electrical Engineering, Universitas Islam Indonesia, Yogyakarta. His research interests include wireless communication, wireless sensor networks, and indoor positioning.

CAHYA DAMARJATI (Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Universitas Gadjah Mada, Yogyakarta, Indonesia, in 2009 and 2015, respectively, and the Ph.D. degree in computer science and information engineering from Asia University, Taichung, Taiwan, in 2022. Since 2015, he has been an Assistant Professor with the Department of Information Technology, Universitas Muhammadiyah Yogyakarta. His research interests include information security, quantum cryptography, computer vision, and artificial intelligence.

ABU BAKAR received the master's degree in medical education from Gadjah Mada University, Yogyakarta, in 2012, and the Ph.D. degree from Da-Yeh University, Taiwan, in 2020. Currently, he is a full-time Lecturer with the Department of Oral Medicine, Baiturrahmah University, Padang, Indonesia, where he also the Head of the Department for Research and Community Services. His research interests include the intersection of dentistry and biotechnology, with specialized expertise in clinical dentistry, biotechnology, and dental materials.

HSING-CHUNG CHEN (Senior Member, IEEE) received the Ph.D. degree in electronic engineering from National Chung Cheng University, Taiwan, in 2007. From February 2008 to July 2018, he was an Assistant Professor and an Associate Professor with the Department of Computer Science and Information Engineering, Asia University, Taiwan. From August 2018 to July 2019, he was a Full Professor with the Department of Computer Science and Information Engineering, Asia University. Since August 2019, he has been a Distinguished Full Professor with the Department of Computer Science and Information Engineering, Asia University. Since May 2014, he has been a Research Consultant with the Department of Medical Research, China Medical University Hospital, China Medical University, Taichung, Taiwan. He has been serving as the Co-Founder of the IEEE Taipei Blockchain Group (Taipei Section), since November 2022. His research interests include information and communication security, cyberspace security, blockchain network security, the Internet of Things application engineering and security, mobile and wireless network protocols, medical and bio-information signal image processing, artificial intelligence and soft computing, and applied cryptography. He is a member of the Taiwan Fuzzy Systems Association (TFSA), ICCIT, CCISA, E-SAM, and IET. He has been awarded the Best Paper Presentation Awards and the Best Post Publications Awards by ACM ICFET2020 and TANET2018, individually. He received the Best Paper Awards from BWCCA2018, MobiSec2017, and BWCCA2016, individually. He received the Best Journal Paper Award from the Association of Algorithm and Computation Theory (AACT). He has been listed in the ''World Ranking of Top 2% Scientists,'' since 2021, created by experts at Stanford University, USA, for three consecutive years (Published dates: October 2021, October 2022, and October 2023). Since February 2017, he has been the Permanent Council Member of the Taiwan Domain Names Association (Taiwan DNA), Taiwan. From August 2019 to July 2020, he was the Head of the Department of Computer Science and Information Engineering, Asia University. He served as the Program Committee Chair for APNIC44 (September 2017) organized by the Asia–Pacific Network Information Centre (APNIC).