Journal of Electronics, Electromedical Engineering, and Medical Informatics
Multidisciplinary: Rapid Review: Open Access Journal Vol. 6, No. 2, April 2024, pp: 182-195; eISSN: 2656-8632

RESEARCH ARTICLE OPEN ACCESS

Manuscript received February 10, 2024; revised February 26, 2024; accepted April 10, 2024; date of publication April 20, 2024
Digital Object Identifier (**DOI**): https://doi.org/10.35882/jeeemi.v6i2.402

How to cite: Manishka Mukhopadhyay, Subhrajyoti Banerjee, Chitrangada Das Mukhopadhyay, Internet of Medical Things and the Evolution of Healthcare 4.0: Exploring Recent Trends, Journal of Electronics, Electromedical Engineering, and Medical Informatics, vol. 6, no. 2, pp. 182-195, April 2024.

Internet of Medical Things and the Evolution of Healthcare 4.0: Exploring Recent Trends

Manishka Mukhopadhyay[1], Subhrajyoti Banerjee[2], Chitrangada Das Mukhopadhyay[2]

[1] Industrial and Systems Engineering, Indian Institute of Technology, Kharagpur, WB, India
[2] Centre of Healthcare Science and Technology, Indian Institute of Engineering Science and Technology, Kharagpur, WB, India
Corresponding author: Chitrangada Das Mukhopadhyay (e-mail: chitrangadam@chest.iiests.ac.in)

ABSTRACT Enhanced patient care and remote health monitoring have always been important issues. Internet of Medical Things (IoMT) is a subsection of Healthcare 4.0 that uses recent technologies like mobile computing, medical sensors, and cloud computing to track patients' medical information in real-time. These data are stored in a cloud computing framework that may be accessed and analyzed by healthcare experts. IoMT and Healthcare 4.0 have immense potential for revolutionizing patient care and diagnostics, despite facing numerous complex challenges. This paper thoroughly analyzes technical, structural, and regulatory obstacles encountered by the healthcare sector. Challenges in IoMT implementation include cost considerations, network stress, interoperability issues, ethical limitations, policy intricacies, security concerns, and vulnerabilities jeopardizing patient privacy. However, amidst these challenges, the study highlights the prospective long-term benefits, including diminished medical costs and enhanced patient care. In this study, we have portrayed a comprehensive exploration of the field of IoMT and different related technologies from more than 100 papers to represent the transformation and growth in this decade. We have illustrated some of the significant findings of applications and innovations in the domain of IoMT. This paper delves into IoMT's application in dementia detection and care, improved data management, fortified cybersecurity measures, and modernizing existing healthcare systems. The study also offers valuable insights into potential mitigation strategies, offered by ongoing research and innovation to address emerging trends and challenges, propelling the trajectory of Healthcare 4.0 towards an optimized and transformative future for patient well-being. Hence future research needs to integrate more prudent technologies addressing challenges including security, privacy, interoperability, and implementation costs.

INDEX TERMS: Cybersecurity measures, dementia detection, Ethics, Healthcare 4.0, IoMT, patient privacy

I. INTRODUCTION

The concept of "Internet of Things (IoT)" refers to the integration of internet connectivity into physical or embedded devices ("things"), enabling them to communicate with other devices, services, and individuals worldwide. This interconnectedness enhances reliability, sustainability, and efficiency through better information accessibility [1]. The IoT has evolved into a sprawling network of interconnected physical objects, facilitating data exchange through the Internet. The exponential growth of IoT has resulted in approximately 10 billion connected devices, with projections soaring to 25 billion by 2025. These "smart" entities, embedded with software, either enhance existing functionalities or introduce new features. Amid this technological revolution, the healthcare sector has witnessed a paradigm shift with the emergence of the Internet of Medical Things (IoMT) [2]. IoMT is a rapidly growing sector of the IoT, and it is attracting increasing interest from researchers because of its extensive potential in Smart Healthcare systems (SHS)[3]. The COVID-19 pandemic witnessed the crucial need for continuous health monitoring during pre- and post-infection stages. IoMT seamlessly stepped into this critical role, enabling remote patient monitoring, screening, and treatment through telehealth[4]. The revenue generated by IoMT-based systems has grown a few billion. This growth trajectory is poised to attract many investors into IoMT-based systems.

While IoMT promises transformative benefits, security remains an issue. The heterogeneous environment of IoT, encompassing devices, protocols, and operating systems, elevates susceptibility to cyber-attacks. The primary motivation for targeting IoMT is the high value of patient data for monitoring and treatment, with the estimated mean cost of IoMT data being 50 times higher than in other sectors. Compounding the challenge, IoMT devices, such as CCTV (closed-circuit television cameras), often lack patch update facilities, necessitating replacement in the face of identified vulnerabilities. Recognizing the imperative nature of security, diverse strategies are employed to ensure the confidentiality and integrity of IoMT-based systems. Symmetric and asymmetric key cryptography are the tools for safeguarding against data leakage. Keyless techniques, such as the use of biometry, blockchain technology, and proxy-based security, play a crucial role in addressing broader security and privacy concerns. These keyless techniques exhibit sensitivity to anomalies in the system, aiding in the detection of both known and novel cyber-attacks.

Rizk, et al. have significantly enhanced IoMT security [5]. Innovative microarchitectures, taxonomic reviews, and generalized IoMT structures have been proposed to improve efficiency, security, and understanding of heterogeneous features in IoMT applications. Integration of advanced technologies such as cloud as well as edge computing and artificial intelligence has been explored to fortify IoMT against evolving cyber threats. Despite these efforts, a comprehensive understanding of the security and privacy aspects of IoMT is still evolving. This paper takes a holistic approach, presenting motivations, security requirements, concerns, and future research directions. It aims to provide a comprehensive understanding of IoMT applications, paving the way for further advancements in this emerging research area.

Healthcare 4.0 signifies a fundamental shift in healthcare systems, driven by digitization and the integration of technologies like the IoT, AI, and cloud computing. This paradigm embraces adjustments in health-management systems, employing cloud computing and mobile communications for continuous and precise clinical image assessments through digitalization. Sun et al. focused on optimizing healthcare resource utilization within existing constraints, particularly in the prompt processing and evaluation of medical big data [6]. Ghubaish et al. proposed innovative security measures for IoMT systems, analyzing potential physical and network threats [7]. Amidst global challenges, such as the COVID-19 pandemic, where healthcare systems face strain, Healthcare 4.0 responds with AI-driven diagnostics and personalized medicine, improving treatment outcomes and healthcare access through telehealth services [8]. IoMT is poised to revolutionize the healthcare sector further and is anticipated to expand with advancements in data analytics, sensor technology, and connectivity. IoMT can connect more devices whether it be medical or lifestyle, enabling early detection of health issues and facilitating early intervention to reduce complications, remote patient care, and real-time monitoring [9]. The symbiosis of IoT, IoMT, and Healthcare 4.0 (FIGURE 1) offers a transformative path towards a future where healthcare is not only accessible but also technologically advanced, ensuring improved outcomes and enhanced quality of life for individuals globally.

This paper aims to comprehensively explore the contribution possibilities of IoMT in healthcare infrastructure and its role in the transition towards Healthcare 5.0. The integration of IoT with healthcare systems necessitates robust security and privacy measures due to the vast amount of data it generates, making it an attractive target for malicious actors. The article also aims to discuss recent research outcomes for seamless integration and data exchange among diverse IoMT devices. Finally, the paper also deals with AI/ML-mediated insights

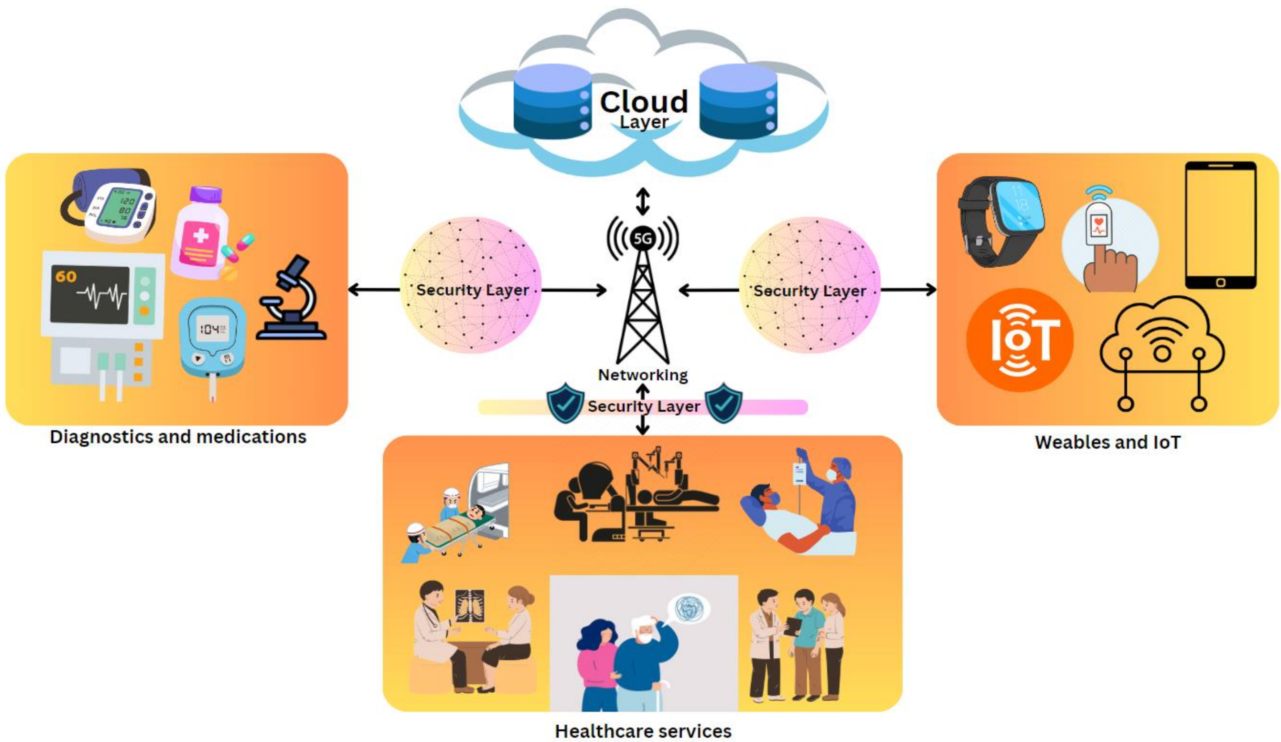

FIGURE 1. IoMT and healthcare infrastructure

into the huge data generated for disease prediction, biomarker identification, and the adoption of IoMT technologies in real-life clinical practice.

A. IoMT transforming healthcare infrastructure

In this comprehensive review, we aim to embark on an exploration of the dynamic intersection between the IoMT and Healthcare 4.0, unraveling the evolution and intricacies of these transformative paradigms.

B. IoMT and prospective security

Beginning with the Evolution of the IoMT, we trace its origins and transformative journey. We then dissect the mechanics of IoMT, elucidating how IoMT works by examining its layers, diverse technologies, and the effective management of interconnected components. Technologies Integrated with IoMT, showcase the fusion of Virtual Reality (VR), Merged Reality (MR), Augmented Reality (AR), networking solutions, Artificial Intelligence (AI), Machine Learning (ML), Big data Visualization, and analytics (BDVA), and Blockchain in shaping the future of healthcare. Highlighting the main aspects and challenges of IoMT and Healthcare 4.0, the review concludes with an examination of the present and future interplay between Healthcare 4.0 and IoMT, providing a holistic perspective on the ongoing transformation in the realm of healthcare.

II. EVOLUTION OF THE IOMT AND HEALTHCARE INDUSTRY

The IoMT evolution marks a transformative era in healthcare, integrating diverse technologies. AI and ML enhance diagnostics and monitor conditions. Blockchain

TABLE 1
Emerging technological confluence in healthcare: a multifaceted integration with IoMT

Technology	Methodology	Purposes	References
Artificial Intelligence /Machine Learning	ML and AI	Diagnostics	[10]
	DL	Computed Tomography scans	[11]
	L-RNN	Forecasting missing data	[12]
	Partial Tree & Random Forest	Brain tumor detection	[13]
	AI/ML	Cardiovascular Disease Monitoring	[14]
	Deep RNN methods	More efficient in terms of latency, error rate, etc.	[15]
	Big-Data	Addressing issues in sustainable ICT	[16], [17]
	AI/ML	Detect DDoS attacks	[18]
Blockchain	Blockchain mediated IoMT	Stress Vigilance	[19]
	Blockchain-based authentication	Decentralization, reliability, and security.	[20]
	Blockchain	Secure management of EHR	[21], [22]
Cryptography	Symmetric and Asymmetric	Security Criteria of Medical Data	[23]
PUF	Host tracking	Tracing in the crowded area.	[24]
	Sensors	Secure physical measurements	[25]
	Devices	Securely monitor patients	[26]
SDN	SDN orchestration	Cyber threats mitigation	[27]
	IoMT cyber training framework	Orthopedic surgery	[28]
	Non-Orthogonal Multiple Access scheduling method	Improved in energy efficiency, network delay	[29]
	IoT-enabled e-healthcare temperance system	Traffic Vigilance	[30]
	IoMT + AI + blockchain	Security management	[31]
CPS	Big data	Mobile healthcare environmental monitoring	[32]
WSN	Public health intelligent systems based on wireless sensor networks	Home care monitoring systems	[33]
Computing Technology	DL	Wearable device for diagnosis	[34]
	Embedded NN Techniques	Healthcare mobile devices	[35]
	Cloud Computing	Healthcare solutions	[36]
	Edge Computing	Healthcare Framework	[37]
	Edge computing + cloud framework	Voice disorder treatments	[38]

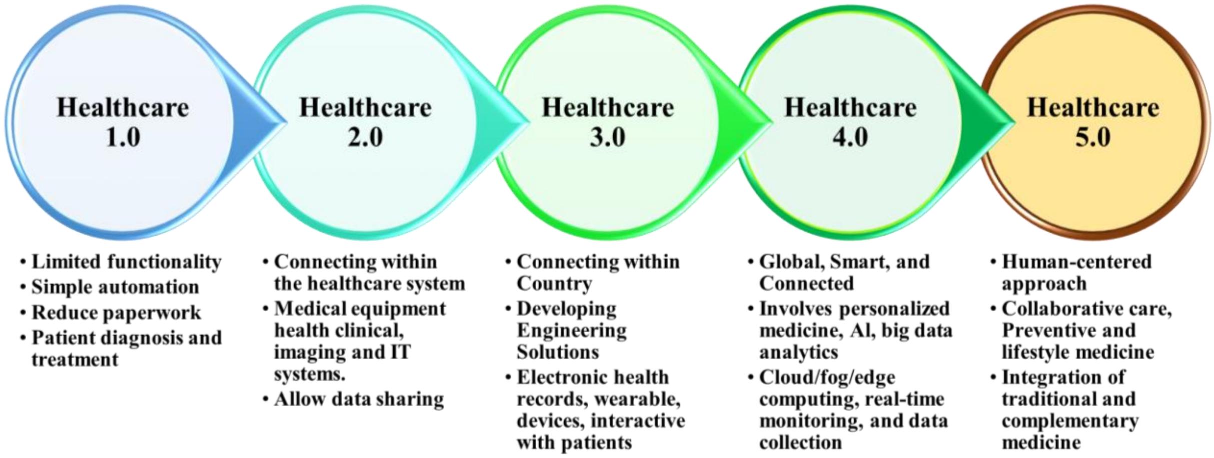

FIGURE 2. Healthcare evolution

ensures secure medical devices and health record management. Cryptography protects sensitive data, while Physical Unclonable Function (PUF) tech enables secure tracking. Software-defined networking (SDN) and IoMT collaborate to manage cyber threats. Cyber-Physical Systems (CPS) monitor environments and Wireless Sensor Networks (WSN) aid public health and home care. This amalgamation (TABLE 1) fosters a connected, efficient, and secure healthcare ecosystem, vital for improved patient care and management. Similarly, in a work by Jabeen et al., an intelligent healthcare system is proposed utilizing Wireless Sensor Networks (WSN) [39]. Nano-sensors collect real-time health data and transmit it to a server. To mitigate concerns regarding time consumption and security, a genetic-based encryption method and an authentication procedure are suggested. Results demonstrate notable enhancements in efficiency and security.

The healthcare industry has undergone a transformative journey, evolving from Healthcare 1.0 to Healthcare 5.0, [41] driven by technological advancements and a focus on patient-centric care. This development anticipates a future where technology seamlessly becomes part of every facet of healthcare, granting patients more control and enhancing outcomes with the adoption of IoMT technologies. Illustrated in FIGURE 2, this evolution delineates the potential development of healthcare, aligning with the transformative capabilities of IoMT.

III. LAYERS OF IoMT: THE SYSTEM ARCHITECTURE

Most IoMTs have three layers namely the things layer, fog layer, and cloud layer as depicted in FIGURE 3. The “things” layer consists of devices directly in contact with the patients, viz., patient monitoring devices, medical records, sensors, pharmacy management tools, and a nutrition plan generator. Data from patient wearables and remote healthcare services are collected in this layer and considered very sensitive. The collected data is then processed further at the fog and cloud layers to derive valuable insights. Healthcare professionals can access patient data via local routers, ensuring fast and efficient healthcare delivery [42]. The fog layer acts as an intermediary between the devices and the cloud layer, comprising local servers as well as gateway devices that form a sparsely distributed fog-networking framework. Utilizing local processing power, it enables real-time responses to users and directs data from servers to the cloud layer. The cloud layer comprises data storage. It provides extensive coverage for integrating large-scale medical and healthcare systems to manage daily operations efficiently[43].

Within this layer, data generated from medical infrastructure is stored and retrieved when required. The Security Layer employs firewalls and encryption to protect against cyber threats [44]. The Application Layer provides access to data for healthcare professionals through electronic health records and apps. The Regulatory Layer ensures compliance with standards like HIPAA (Health Insurance Portability and Accountability Act.) and GDPR (General Data Protection Regulation), establishing a secure IoMT framework [45], [46].

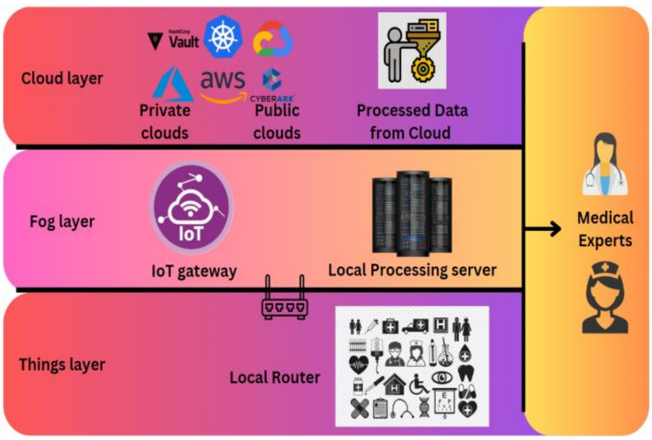

FIGURE 3. The interconnections of layers and medical experts

IV. ADVANCED SENSORS AND IOMT INTEGRATION FOR PERSONALIZED PATIENT CARE

IoMT applications rely on distinct sensor types within the architecture. They can be categorized as Disposable sensors, connected sensors, market cap sensors, and miscellaneous sensors. Disposable e-health sensors like MAX30205 and

MLX90614 respond to parameters such as temperature and pressure [47]. Connected e-health sensors maintain continuous connectivity, ensuring consistent communication [48]. IoMT market cap sensors like Kardia Heart (KH) and Smart Thermometer (ST) are prominent for home-based health monitoring, including wearable fitness sensors. Specialized miscellaneous sensors focus on the well-being of gravid women. The Internet of DNA (IoDNA) is pivotal for predicting genetic defects in newborns, representing a milestone in advanced medication systems and genome mapping. TABLE 2 provides a summary of their costing and product aspects.

V. IMPORTANT TECHNOLOGIES USED FOR IoMT

A. BLOCKCHAIN TECHNOLOGY

It embodies the potential to revolutionize healthcare by securely storing and transferring patient data through a resistant to modification chain. It ensures accuracy, transparency, and security in managing medical records, reducing errors, and improving data security. Essential elements include data provenance, decentralized management, robustness, security, and privacy [49]. Blockchain plugin technology establishes a secure and immutable connection among data repositories. An example is 'MedBlock,' which provides highly secure access control for efficient Electronic Medical Record (EMR) access. 'Healthcare Data Gateway (HDG)' by Yue et al. leverages blockchain for privacy-compliant patient information sharing [50]. In the context of combating COVID-19, 'CoviChain' facilitates secure data transfer of infected persons to the hospital system using edge infrastructure [51]. Alsamhi et al. implemented a blockchain configuration for multi-robot and decentralized multi-drone systems addressing COVID-19 challenges [52].

B. PHYSICALLY UNCLONABLE FUNCTION (PUF)

PUF devices generate unique fingerprints or cryptographic keys for vulnerable elements. These distinctive fingerprints or signatures result from variations in the fabrication process of these devices. enhancing the security of devices particularly when the end devices, such as sensors, are susceptible to hardware tampering attacks [53].

C. ARTIFICIAL INTELLIGENCE (AI)

AI/Machine Learning (ML) and Natural Language Processing (NLP), are integral parts of IoMT and Healthcare 4.0, particularly in precision medicine and various healthcare applications. AI facilitates real-time solutions, analyzing historical and current data for personalized treatment plans, diagnostics, and decision-making processes [54]. AI-based classifiers can automate tasks such as patient information capture, appointment scheduling, lab test determination, treatment planning, medication recommendations, and surgical procedures. NLP assists in extracting information from unstructured data, such as lab reports and examination notes. In Healthcare 4.0, AI revolutionizes diagnostics through the analysis of medical images, patient data, and genetic information. It expedites drug discovery by predicting pharmaceutical compound efficacy and identifying potential lead compounds. AI also enhances remote monitoring, enabling prompt intervention based on detected anomalies. AI-powered chatbots and virtual assistants are very popular. Disease prediction, telesurgery, and real-time communication in Healthcare 4.0 leverage AI, transforming healthcare delivery and patient care.

D. SOFTWARE-DEFINED NETWORKING (SDN)

SDN divides IoMT network architecture into the data plane and control plane components. The data plane forwards traffic, while the control plane enables informed decision-making. SDN, with standardized protocols like OpenFlow, Open Switch Database Management Protocol, and OF-CONFIG, facilitates interaction between the data and control planes. Through standardized interfaces, data from the IoMT's data plane can be collected externally, potentially from a cloud-based server using OpenFlow, enabling various e-healthcare applications [55]. Similarly, in a work by Rahaman et.al.[56]present a patient-centric agent-based medical framework for IoMT networks, focusing on information security and utilizing Hyperledger Fabric Network for secure data maintenance and communication. They propose a mobile application for easy adaptation of the

Table 2:
Commercial Biosensors used in IoMT and their respective usage

Product	Cost	Disease/ Monitoring	Type of Sensor	Reference
Proteus Digital Monitor	Very high	Diabetes and Hypertension	Clinical biometric	https://www.proteus.com/
OM signal	High	Wellness care	Brain and fitness	http://omsignal.com/
Thalmic Labs	High	Virtual reality of health status	Home monitoring	https://www.bynorth.com/
BabyBe	High	Biosignal between mother and premature infant	Sleep, infant, and woman care	http://www.babybemedical.com/
AdhereTech	Low	Regular medication	Clinical	https://www.adheretech.com/
CYCORE	Average	Cancer	Clinical Biometric	http://cycore.ucsd.edu/
Halo Neuroscience	Average	Cognitive task management	Brain and fitness	https://www.haloneuro.com/
Volunits	Very High	Cancer self-management	Clinical	https://www.voluntis.com/

model, enabling convenient access to healthcare services and facilitating remote healthcare monitoring. In FIGURE 4, SDN-enabled IoMT architecture IoMT devices are shown to connect to e-healthcare applications, potentially in the cloud, using the SDN control plane at the fog layer. The control plane aggregates IoMT device data for specific areas like security, privacy, patient diagnosis, or safety. The northbound interface is crucial for communication between the SDN control plane and AI applications, allowing data collection and command implementation onto IoMT devices.

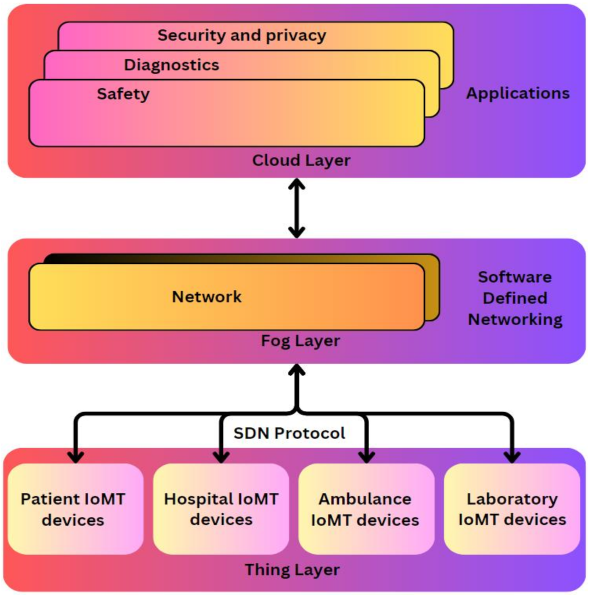

FIGURE 4: The Architectural structure of SDN with Fog and Cloud layers in IoMT.

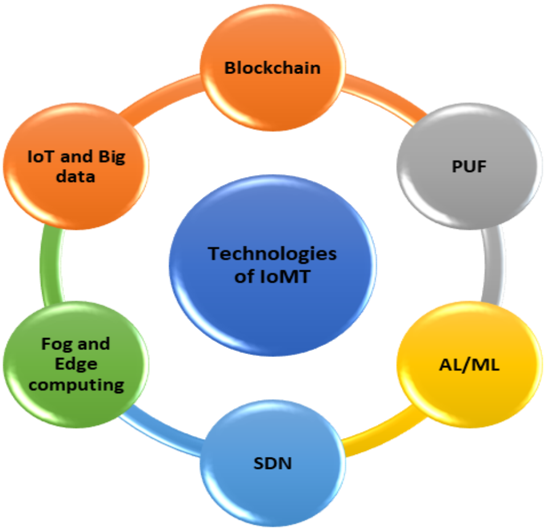

Figure 5. Representation of different technologies in IoMT

E. FOG COMPUTING AND EDGE COMPUTING

Healthcare cloud computing provides access to a shared pool of customizable resources, streamlining rapid provisioning and release with minimal management involvement. It securely stores, processes, and shares medical data in the cloud, offering a cost-effective solution that promotes seamless collaboration and accessibility to data from anywhere at any time. Fog computing integrates cloud computing into the IoT, decentralizing data processing for improved response times and reduced latency, providing flexibility in data processing operations, and allowing rapid adaptation to changing demands [57]. Edge computing (FIGURE 5) minimizes network latency by locally processing data instead of transmitting it to a cloud-based server. This enhances processing speed, reduces costs, and improves the security of patient data. Edge computing enables the storage of large data volumes closer to the network edge, facilitating faster and more secure data processing [58].

F. VIRTUAL, MIXED, AND AUGMENTED REALITY

Virtual, Mixed, and Augmented Reality (VR, MR, and AR) offer a wide range of applications within the Internet of Medical Things (IoMT) framework, spanning clinical/therapeutic, business/industry, and education/training domains in healthcare. VR aids in treating mental health conditions such as anxiety disorders, stress, and PTSD through exposure therapy and relaxation techniques, and enables customized rehabilitation programs for motor skill recovery and cognitive training. VR distracts patients from pain sensations by immersing them in engaging virtual environments, reducing the need for analgesics. It also facilitates lifestyle interventions by simulating healthy behaviors and promoting physical activity and assists in monitoring patients undergoing cancer treatment, providing immersive experiences for distraction during chemotherapy sessions [59]. AR superimposes computer-generated images onto the real world and is beneficial for visualizing invisible concepts, annotating navigation, and reducing stress and anxiety in quarantined patients [60]. In medical training, Fundamental VR provides simulation training for surgeons, XVision Augmedics incorporates 3D representation for an X-ray vision-like effect [61], and Oxford VR focuses on alleviating fear and other attributes associated with mental disorders[62]. These applications showcase the broad impact of immersive technologies in the healthcare sector within the IoMT framework.

FIGURE 6. Comprehensive characteristics of BDVA

G. BIG DATA VISUALIZATION AND ANALYTICS

Big Data involves the collection, storage, and analysis of vast datasets to gain insights into patient care and health outcomes. Data-driven analytics and machine learning help in the prediction of early diagnoses, treatment plans, and medication choices [63]. Big Data Visualization and Analytics (BDVA) has emerged as a crucial tool for analyzing the substantial volume of data generated by IoMT devices. BDVA collects data from wearable sensors, climate, temperature, environment, location, and medical sources, presenting it in structured, unstructured, and semi-structured formats [64]. Cloud computing integrates and visualizes the data, while database analytics processes it for extraction, cleaning, and statistical analysis before use by doctors or remotely [65]. BDVA principles are encapsulated in the "V's" of big data analytics as shown in FIGURE 6 [66]. Visualization and Visibility are pivotal in the coherent representation and accessibility of healthcare insights, while Virality acknowledges the transformative potential of medical data. The Virtual dimension integrates intelligence into IoMT datasets, fostering innovation and optimizing patient-centric healthcare paradigms.

VI. THE TREND AND APPLICATION OF HEALTHCARE 4.0 AND IoMT

A. DRONES AND ROBOTICS

Drones serve as versatile and cost-effective tools in healthcare, efficiently delivering medical supplies to remote areas and enhancing emergency services. They are crucial in mass testing, surveillance, and medical deliveries during global health challenges. Diagnostic drones equipped with thermal imaging contribute to early infection detection. Additionally, drones are deployed for efficient disinfection, showcasing their potential to revolutionize medical logistics and emergency response systems, improving healthcare delivery [67], [68]. The integration of robotics in smart healthcare applications represents a transformative advancement, enhancing diagnostic precision and enabling swift responses to medical emergencies. Robots automate routine tasks, streamline operations, and improve efficiency while safeguarding healthcare workers. Despite benefits, there are risks, including over-reliance on technology [69]. Striking a balance between technological integration and human-centric care is crucial for preserving the quality of patient care. Comprehensive risk management strategies are necessary to address potential malfunctions and errors in healthcare settings [58, 59].

B. SMART HOMES

Assisted living, an important form of long-term care, supports elderly as well as disabled individuals with daily activities, promoting comfort and minimizing hospitalization [72]. Telepresence and videoconferencing robotic solutions ensure continuous monitoring, fostering communication, and offering educational and therapeutic activities [73]. Integrating AI into ambient intelligence systems enhances data processing, enabling automatic alerts and emergency assistance [74]. Smart homes with IoT devices revolutionize healthcare through IoMT integration, monitoring vital health data. Smart Healthcare at Home (SHAH) combines Digital Twins, IoMT, and AI for real-time monitoring and safety [75]. IoMT-based remote patient monitoring faces challenges, yet breakthroughs in wearable technology, AI, edge computing, and 5G are propelling Healthcare 4.0 systems, transforming healthcare delivery [76]. In summary, IoT and IoMT integration in smart homes bring personalized healthcare, while ongoing advancements shape the trajectory of Healthcare 4.0 systems. Smart home environments with IoMT devices enable personalized medical care, reducing the need for hospitalization.

C. PERSONALISED HEALTHCARE AND DIGITAL TWINS

Personalized healthcare utilizes technology to tailor medical treatments to individual patient characteristics, incorporating data on medical history, lifestyle, and genetics to design customized treatment plans [77]. Digital Twins (DT), initially used in industrial manufacturing, are now integrated into healthcare, notably in the IoMT context [78]. DT models optimize medical resource allocation, aiding in personnel, equipment, and appointment management. These models also assist in understanding patient needs and predicting future trends, proving valuable during crises like the COVID-19 pandemic. In healthcare, Digital Organs create models based on extensive medical data to investigate hypotheses and improve services without human experimentation [79]. AI/ML methods are used to train models for reliable predictions and diagnoses.

D. REHABILITATION

The integration of IoMT technologies into smart rehabilitation systems is facilitated through an ontology-based automated design method [80]. This approach ensures efficient remote consultations within comprehensive rehabilitation programs. Notable examples include an integrated application system designed for correctional facilities, a medical rehabilitation system tailored for smart cities [69, 70], and a language training system designed to support children with autism. These IoMT-based rehabilitation systems showcase the versatility and potential impact of smart healthcare services in improving accessibility, personalization, and efficiency within the realm of physical medicine.

E. TELEMEDICINE AND MANAGEMENT SERVICES

The IoMT has transformed healthcare management, particularly in chronic disease care. Continuous monitoring through IoMT allows early intervention, such as with COPD patients monitored via smartphone platforms, which detect exacerbation signs and reduce hospitalizations [83]. IoMT improves medication management systems, ensuring accurate prescription, administration, and documentation, with examples like intelligent packaging and RFID tags enhancing medication control. Additionally, IoMT facilitates telemedicine, granting access to medical data from various locations, and offering real-time drug monitoring and personalized dosing through innovations like smart pills. In wheelchair management, IoMT enhances patient safety and efficiency by providing safe movement, reducing risks of falls, and optimizing staff time. IoT-based wheelchair healthcare systems demonstrate IoMT's potential in evaluating location accessibility through vital signs and environmental data, enhancing patient care, safety, and efficiency. Notable healthcare apps like Aarogya Setu for COVID-19 contact tracing and Beat-O for diabetes management exemplify the evolving digital health landscape, while alternative devices like One or Fitbit's Zip regale to fitness tracking independently of smartphones, addressing diverse user preferences [84].

F. IoMT-DRIVEN CONTINUOUS HEALTH MONITORING

Continuous health monitoring, driven by the IoMT, is transforming healthcare by providing real-time insights into patients' vital signs, reducing unnecessary doctor visits, and enabling personalized treatment plans [85]. Wearable multi-parameter continuous cardiac monitoring systems are particularly valuable for managing chronic conditions like diabetes, diabetic retinopathy, and heart diseases, ensuring ongoing health surveillance [86], [87]. Despite IoMT's potential, concerns about privacy and safety risks persist, especially with health data transmission. However, IoMT adoption has improved patient and healthcare provider experiences, particularly through remote patient monitoring, facilitating timely care delivery and real-time health assessments. Continuous glucose monitoring, like, Dexcom Continuous Glucose Monitoring and DexcomG7 (pediatric), key IoMT components, revolutionizes diabetes management by automating glucose level monitoring and issuing alerts for deviations [40]. While IoMT-driven continuous health monitoring holds promise, careful attention to privacy, security, and potential risks is crucial.

Continuous monitoring of depression and mood using IoT devices empowers individuals to recognize triggers and manage mental health proactively. Clinicians benefit from tracking depression and mood data over time, enabling personalized treatment plans and collaboration with mental health professionals, enhancing understanding of depression's long-term effects [88]. Monitoring Parkinson's disease progression through IoT devices provides valuable insights for doctors, facilitating adjustments to treatment plans and leading to the identification of more effective therapies. Utilizing IoT devices for monitoring movements and behavioral changes enables informed adjustments to therapies, optimizing disease management and improving patient outcomes in Parkinson's disease [89].

G. DEMENTIA AND MANAGING EARLY SIGNS OF COGNITIVE DECLINE

As a network of interconnected devices and applications, the IoMT serves as a healthcare-focused extension, providing timely support to patients through wired or wireless connections. This significantly enhances healthcare infrastructure and improves quality of life. Catarinucci et al. [90] introduced a real-time smart hospital system based on IoT, utilizing wireless sensor networks and mobile devices interconnected through REST architecture. Patient data collected by this system is transmitted to a central repository, accessible via a monitoring app. Islam et al. [91] explored diverse IoT-based healthcare architectures, emphasizing applications in child and elderly care, and utilizing various medical sensors for patient monitoring. Baker et al. [92] proposed an IoT-based healthcare model applicable to routine outpatient department (OPD) visits and emergency medical conditions. Dziak et al. [93] suggested an IoT-based home care system for the elderly, focusing on those with health or memory issues. These examples showcase the diverse applications of IoT and IoMT in healthcare, reflecting efforts to enhance patient care and well-being. Specific research initiatives also target early detection and monitoring of neurodegenerative conditions like dementia and Parkinson's disease, utilizing IoT technologies for early detection and personalized care approaches.

H. APPLICATIONS OF AI/ML AND IoMT

Jiang et al. (2017) highlighted AI applications in various diseases, including cancers, nervous system disorders, cardiovascular issues, urogenital conditions, pregnancy-related concerns, digestive disorders, respiratory issues, skin conditions, and endocrine/nutritional disorders [94]. Pantanowitz et al. (2020) developed AI algorithms for detecting and evaluating digitized slides of prostate core needle biopsies [95]. IBM Watson, as demonstrated by Somashekhar et al. [96], showed reliability in cancer diagnosis. Esteva et al. (2017) employed AI to analyze clinical images and identify skin cancer subtypes. Bouton et al. (2018) created an AI system for quadriplegic patients to restore movement control [85, 86]. AI applications extend to controlling upper-limb prostheses, improving congenital anomaly diagnosis accuracy, diagnosing heart disease through cardiac images, automating ventricle segmentations with 'Arterys' Cardio DL, diagnosing gastric cancer based on abnormal genetic expression of long non-coding RNAs, and localizing neural injuries using electrodiagnosis support systems, as developed by Shin et al. These advancements highlight AI's multifaceted role in enhancing healthcare diagnosis and treatment [99].

VII. THREATS IN IoMT COMMUNICATIONS PROTOCOL AND MITIGATION STRATEGIES

In the perception layer, various communication technologies, including Infrared (IR), RFID, Near Field Communication (NFC), Bluetooth/BLE, and Z-Wave, present inherent security challenges that can be susceptible to compromise. IR communications lack embedded security controls, exposing vulnerabilities if an attacker intercepts the IR beam, though this threat can be mitigated by requiring proximity [100]. RFID communications, despite widespread use, often lack inherent protection for embedded data. RFID implementations can be strengthened through symmetric key encryption or signature-based integrity control. NFC security employs protocols for key exchange, data encryption, and integrity checks using the Advanced Encryption Standard (AES) algorithm, introducing unique security considerations for each operational mode [101]. Wearable devices, like smartwatches acting as pulse oximeters, are vulnerable due to Bluetooth communication protocols. Attackers can gain unauthorized access by pairing with the device during data transmission to a smartphone, accessing sensitive medical data due to the lack of authentication between connections. Strengthening authentication processes and avoiding automatic pairing are crucial to mitigate such threats. Bluetooth/BLE, in a secure simple pairing (SSP) in mode 4 can enhance service-level security, mitigating Man-In-The-Middle (MITM) attacks through encryption based on device-specific identifiers [102]. Z-Wave protocols incorporate encryption and behavior detection, ensuring data confidentiality and integrity through AES encryption and shared keys. Monitoring devices, including cameras and alarm systems, are susceptible to hacking. Protection involves advanced intrusion detection systems and robust authentication protocols to detect and prevent misuse or interference with patient care. COAP and MQTT protocols, primarily at the application layer, are at risk, emphasizing the need for comprehensive security measures across all IoMT communication layers [103].

VIII. CHALLENGES AND PROSPECTS: HEALTHCARE 4.0 AND IOMT

IoMT encounters technological limitations, emphasizing the need to overcome challenges in accurate data acquisition, interoperability, bandwidth constraints, service quality, extended battery life, and sensor compatibility (FIGURE 7). Advances in wearable technology, AI, edge computing, and 5G are critical drivers for overcoming limitations and enhancing IoMT effectiveness in healthcare [104]. IoMT implementation incurs significant costs, covering hardware, software, and data management, with long-term benefits of reduced medical costs and improved outcomes. Network stress arises due to healthcare organizations lacking seamless IoMT device integration infrastructure. Interoperability demands standardization for smooth data exchange. Ethical concerns on patient data privacy accompany IoMT, urging a balance between leveraging data for healthcare and privacy protection [105].

The World Health Organization (WHO) has launched a Global Strategy on Digital Health 2020–2025 aimed at bolstering health systems globally through digital health technologies, with a focus on empowering patients, health professionals, and healthcare providers toward achieving universal health coverage. Across various regions, countries have embraced digital health policies, such as the European Union's reinforcement of privacy laws through GDPR since May 2018. In Asia, particularly Southeast and East Asia, countries like Singapore, South Korea, and Thailand have witnessed remarkable strides in digital healthcare adoption. However, India faces hurdles in implementing widespread digitization due to capacity shortages, rural transportation challenges, financial constraints, and social stigmas surrounding certain health conditions. Indian officials are insisting on a growing call for a clear and comprehensive data protection framework, as advocated by former Supreme Court justice B. N. Srikrishna, emphasizing the need to prevent arbitrary government interventions. Moreover, in light of high out-of-pocket healthcare expenses in India, it is imperative for the government to prioritize the development of such a framework and invest in enhancing infrastructure, personnel, and facilities to ensure widespread access to affordable and user-friendly digital healthcare services for the population[106].

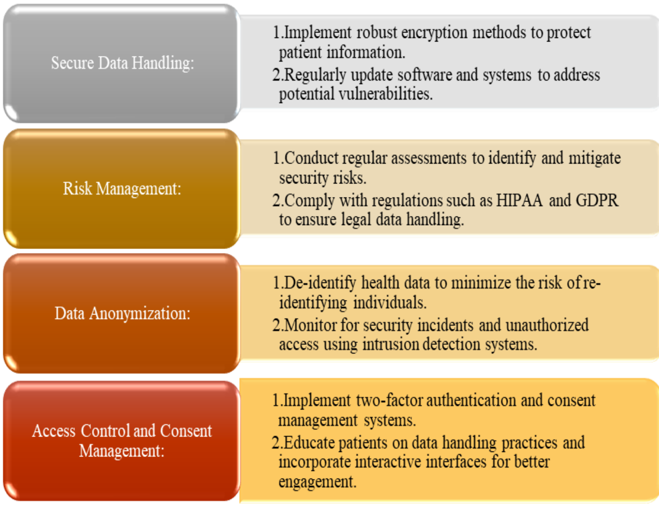

FIGURE 7. **The challenges and possible mitigation strategies in IoMT implementation and execution**

Policies and standardization issues complicate IoMT progress, with efforts for unified policies. Security vulnerabilities necessitate secure databases and regular updates. Challenges specific to IoMT in dementia care include processing vast healthcare data, network security, outdated infrastructure, and lacking standard IoMT equipment. Addressing these challenges is crucial for unlocking IoMT's full potential in healthcare [107].

IX. CONCLUSIONS

The integration of the IoMT and Healthcare 4.0 promises a revolutionary impact on healthcare services, emphasizing advancements in hardware, communication technology, and transformative applications. Despite the potential for enhanced proactivity and efficiency, critical concerns related to data security, privacy, and implementation challenges must be addressed for the full realization of benefits. Challenges persist, including the cost of IoMT implementation, network stress, interoperability issues, ethical considerations, and security vulnerabilities. Addressing these challenges requires substantial investment, upgraded infrastructure, standardization efforts, and robust cybersecurity measures. In the realm of IoMT applications in dementia, innovative solutions show promise in early detection and personalized care, necessitating ongoing research and modernization efforts. Collaboration between stakeholders, ongoing research, and commitment to addressing challenges is imperative for fully realizing the potential of IoMT in revolutionizing healthcare delivery. Emerging technologies such as AI, virtual reality, and advanced connectivity, along with Blockchain and Software-Defined Networking, are central to mitigating vulnerabilities. Future research directions aim to refine and advance these technologies to improve global healthcare outcomes. The complexity of the IoMT networks means no single network protocol can meet the diverse requirements of the various setups. Different healthcare settings demand distinct approaches to data processing, communication, and device interconnectivity. Holistic solutions, encompassing infrastructure upgrades, advanced processing techniques, and responsible frameworks, are essential for the ethical and efficient transformation of healthcare delivery through Healthcare 4.0 and IoMT. The swift integration of IoMT technologies within the healthcare industry indicates a growing trend toward more complex and expansive use of Wireless Sensor Networks (WSN) and sensor networks in medical services.

ACKNOWLEDGMENTS

The authors appreciate the cooperation and positive inputs provided by members of the Neuroscience Laboratory of the Centre for Healthcare Science and Technology, IIEST.

REFERENCES

[1] S. C. Mukhopadhyay and N. K. Suryadevara, "Internet of Things: Challenges and Opportunities," *Internet of Things*, vol. 9, pp. 1–17, 2014, doi: 10.1007/978-3-319-04223-7_1.

[2] S. Al-Sarawi, M. Anbar, R. Abdullah, and A. B. Al Hawari, "Internet of things market analysis forecasts, 2020-2030," *Proceedings of the World Conference on Smart Trends in Systems, Security and Sustainability, WS4 2020*, pp. 449–453, Jul. 2020, doi: 10.1109/WORLDS450073.2020.9210375.

[3] R. Dwivedi, D. Mehrotra, and S. Chandra, "Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review," *J Oral Biol Craniofac Res*, vol. 12, no. 2, pp. 302–318, 2022, doi: 10.1016/j.jobcr.2021.11.010.

[4] A. M. Arif, A. M. Hamad, and M. M. Mansour, "Internet of (Healthcare) Things Based Monitoring for COVID-19+ Quarantine/ Isolation Subjects Using Biomedical Sensors, A Lesson from the Recent Pandemic, and an Approach to the Future.," *Journal of Electronics, Electromedical Engineering, and Medical Informatics*, vol. 5, no. 1, pp. 1–12, Jan. 2023, doi: 10.35882/JEEEMI.V5I1.267.

[5] D. Rizk, R. Rizk, and S. Hsu, "Applied Layered-Security Model to IoMT," in *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, IEEE, Jul. 2019, pp. 227–227. doi: 10.1109/ISI.2019.8823430.

[6] 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, doi: 10.1109/access.2020.2997831.

[7] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. K. Al-Ali, and R. Jain, "Recent Advances in the Internet of Medical Things (IoMT) Systems Security," *IEEE Internet Things J*, vol. 8, no. 11, p. 1, 2020, doi: 10.1109/jiot.2020.3045653.

[8] A. Gupta and A. Singh, "Healthcare 4.0: recent advancements and futuristic research directions," *Wirel Pers Commun*, 2022, doi: 10.1007/s11277-022-10164-8.

[9] M. Osama *et al.*, "Internet of Medical Things and Healthcare 4.0: Trends, Requirements, Challenges, and Research Directions," *Sensors*, vol. 23, no. 17, p. 7435, 2023, doi: 10.3390/s23177435.

[10] S. Lalmuanawma, J. Hussain, and L. Chhakchhuak, "Applications of machine learning and artificial intelligence for Covid-19 (SARS-CoV-2) pandemic: A review," *Chaos Solitons Fractals*, vol. 139, p. 110059, 2020, doi: 10.1016/j.chaos.2020.110059.

[11] A. Sedik, M. Hammad, Fathi, B. B. Gupta, and A. A. Abd, "Efficient deep learning approach for augmented detection of Coronavirus disease," *Neural Comput Appl*, vol. 34, no. 14, pp. 11423–11440, 2021, doi: 10.1007/s00521-020-05410-8.

[12] H. Turabieh, Amer, and N. Abu-El-Rub, "Dynamic L-RNN recovery of missing data in IoMT applications," *Future Generation Computer Systems*, vol. 89, pp. 575–583, 2018, doi: 10.1016/j.future.2018.07.006.

[13] S. R. Khan, M. Sikandar, A. Almogren, I. U. Din, A. Guerrieri, and G. Fortino, "IoMT-based computational approach for detecting brain tumor," *Future Generation Computer Systems*, vol. 109, pp. 360–367, 2020, doi: 10.1016/j.future.2020.03.054.

[14] A. Kilic, "Artificial Intelligence and Machine Learning in Cardiovascular Health Care," *Ann Thorac Surg*, vol. 109, no. 5, pp. 1323–1329, 2020, doi: 10.1016/j.athoracsur.2019.09.042.

[15] H. Song, J. Bai, Y. Yi, J. Wu, and L. Liu, "Artificial Intelligence Enabled Internet of Things: Network Architecture and Spectrum Access," *IEEE Comput Intell Mag*, vol. 15, no. 1, pp. 44–51, 2020, doi: 10.1109/mci.2019.2954643.

[16] J. Wu, S. Guo, J. Li, and D. Zeng, "Big Data Meet Green Challenges: Greening Big Data," *IEEE Syst J*, vol. 10, no. 3, pp. 873–887, 2016, doi: 10.1109/jsyst.2016.2550538.

[17] J. Wu, S. Guo, J. Li, and D. Zeng, "Big Data Meet Green Challenges: Big Data Toward Green Applications," *IEEE Syst J*, vol. 10, no. 3, pp. 888–900, 2016, doi: 10.1109/jsyst.2016.2550530.

[18] N. Gautam *et al.*, "Artificial Intelligence, Wearables and Remote Monitoring for Heart Failure: Current and Future Applications," *Diagnostics*, vol. 12, no. 12, p. 2964, 2022, doi: 10.3390/diagnostics12122964.

[19] L. Rachakonda, A. K. Bapatla, S. P. Mohanty, and E. Kougianos, "SaYoPillow: Blockchain-Integrated Privacy-Assured IoMT Framework for Stress Management Considering Sleeping Habits," *IEEE Transactions on Consumer Electronics*, vol. 67, no. 1, pp. 20–29, 2021, doi: 10.1109/tce.2020.3043683.

[20] F. Fotopoulos, V. Malamas, T. K. Dasaklis, P. Kotzanikolaou, and C. Douligeris, "A Blockchain-enabled Architecture for IoMT Device Authentication," *2020 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE)*, 2020, doi: 10.1109/ecice50847.2020.9301913.

[21] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?," *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, 2018, doi: 10.1109/mcc.2018.011791712.

[22] F. Girardi, G. De Gennaro, L. Colizzi, and N. Convertini, "Improving the Healthcare Effectiveness: The Possible Role of EHR, IoMT and Blockchain," *Electronics (Basel)*, vol. 9, no. 6, p. 884, 2020, doi: 10.3390/electronics9060884.

[23] M. Noura, "Efficient and secure cryptographic solutions for medical data," *Hal.science*, 2019, doi: https://theses.hal.science/tel-02945773.

[24] V. P. Yanambaka, A. Abdelgawad, and K. Yelamarthi, "PIM: A PUF-Based Host Tracking Protocol for Privacy Aware Contact Tracing in Crowded Areas," *IEEE Consumer Electronics Magazine*, vol. 10, no. 4, pp. 90–98, 2021, doi: 10.1109/mce.2021.3065215.

[25] H. Ma, Y. Gao, O. Kavehei, and D. C. Ranasinghe, "A PUF sensor: Securing physical measurements," 2017, doi: 10.1109/percomw.2017.7917639.

[26] M. Masud *et al.*, "A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care," *IEEE Internet Things J*, vol. 8, no. 21, pp. 15694–15703, 2021, doi: 10.1109/jiot.2020.3047662.

[27] S. Liaqat, A. Akhunzada, F. S. Shaikh, A. Giannetsos, and M. A. Jan, "SDN orchestration to combat evolving cyber threats in Internet of Medical Things (IoMT)," *Comput Commun*, vol. 160, pp. 697–705, 2020, doi: 10.1016/j.comcom.2020.07.006.

[28] J. Cecil, A. Gupta, M. Pirela-Cruz, and P. Ramanathan, "An IoMT based cyber training framework for orthopedic surgery using Next Generation Internet technologies," *Inform Med Unlocked*, vol. 12, pp. 128–137, 2018, doi: 10.1016/j.imu.2018.05.002.

[29] Z. Askari, J. Abouei, M. Jaseemuddin, and A. Anpalagan, "Energy-Efficient and Real-Time NOMA Scheduling in IoMT-Based Three-

Tier WBANs," *IEEE Internet Things J*, vol. 8, no. 18, pp. 13975–13990, 2021, doi: 10.1109/jiot.2021.3069659.
[30] S. Badotra, D. Nagpal, S. N. Panda, S. Tanwar, and S. Bajaj, "IoT-Enabled Healthcare Network With SDN," 2020, doi: 10.1109/icrito48877.2020.9197807.
[31] H. Mohd, W. H. Hassan, S. Sameen, Z. S. Attarbashi, M. Alizadeh, and L. A. Latiff, "IoMT amid COVID-19 pandemic: Application, architecture, technology, and security," *Journal of Network and Computer Applications*, vol. 174, p. 102886, 2021, doi: 10.1016/j.jnca.2020.102886.
[32] R. Atat, L. Liu, J. Wu, G. Li, C. Ye, and Y. Yang, "Big Data Meet Cyber-Physical Systems: A Panoramic Survey," *IEEE Access*, vol. 6, pp. 73603–73636, 2018, doi: 10.1109/access.2018.2878681.
[33] P. Magaña-Espinoza *et al.*, "WiSPH: A Wireless Sensor Network-Based Home Care Monitoring System," *Sensors*, vol. 14, no. 4, pp. 7096–7119, 2014, doi: 10.3390/s140407096.
[34] A. Ahila, F. Dahan, R. Alroobaea, W. Y. Alghamdi, F. Hajjej, and K. Raahemifar, "A smart IoMT based architecture for E-healthcare patient monitoring system using artificial intelligence algorithms," *Front Physiol*, vol. 14, 2023, doi: 10.3389/fphys.2023.1125952.
[35] A. Poniszewska-Maranda, D. Kaczmarek, N. Kryvinska, and F. X. Xhafa, "Studying usability of AI in the IoT systems/paradigm through embedding NN techniques into mobile smart service system," *Computing*, vol. 101, no. 11, pp. 1661–1685, 2018, doi: 10.1007/s00607-018-0680-z.
[36] G. Muhammad, M. Rahman, A. Alelaiwi, and A. Alamri, "Smart Health Solution Integrating IoT and Cloud: A Case Study of Voice Pathology Monitoring," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 69–73, 2017, doi: 10.1109/mcom.2017.1600425cm.
[37] T. Muhammed, R. Mehmood, A. Albeshri, and I. Katib, "UbeHealth: A Personalized Ubiquitous Cloud and Edge-Enabled Networked Healthcare System for Smart Cities," *IEEE Access*, vol. 6, pp. 32258–32285, 2018, doi: 10.1109/access.2018.2846609.
[38] G. Muhammad, M. F. Alhamid, M. Alsulaiman, and B. Gupta, "Edge Computing with Cloud for Voice Disorder Assessment and Treatment," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 60–65, 2018, doi: 10.1109/mcom.2018.1700790.
[39] T. Jabeen, I. Jabeen, H. Ashraf, N. Z. Jhanjhi, A. Yassine, and M. S. Hossain, "An Intelligent Healthcare System Using IoT in Wireless Sensor Network," *Sensors 2023, Vol. 23, Page 5055*, vol. 23, no. 11, p. 5055, May 2023, doi: 10.3390/S23115055.
[40] J. L. Ausín, J. Ramos, A. Lorido, P. Molina, and J. F. Duque-Carrillo, "Wearable and Noninvasive Device for Integral Congestive Heart Failure Management in the IoMT Paradigm," *Sensors*, vol. 23, no. 16, p. 7055, 2023, doi: 10.3390/s23167055.
[41] J. Basulo-Ribeiro and L. Teixeira, "The Future of Healthcare with Industry 5.0: Preliminary Interview-Based Qualitative Analysis," *Future Internet*, vol. 16, no. 3, p. 68, 2024, doi: 10.3390/fi16030068.
[42] C. Li, J. Wang, S. Wang, and Y. Zhang, "A review of IoT applications in healthcare," *Neurocomputing*, vol. 565, p. 127017, Jan. 2024, doi: 10.1016/J.NEUCOM.2023.127017.
[43] F. Khan, M. A. Jan, R. Alturki, M. D. Alshehri, S. T. Shah, and A. U. Rehman, "A Secure Ensemble Learning-Based Fog-Cloud Approach for Cyberattack Detection in IoMT," *IEEE Trans Industr Inform*, vol. 19, no. 10, pp. 10125–10132, Oct. 2023, doi: 10.1109/TII.2022.3231424.
[44] F. Kamalov, B. Pourghebleh, M. Gheisari, Y. Liu, and S. Moussa, "Internet of Medical Things Privacy and Security: Challenges, Solutions, and Future Trends from a New Perspective," *Sustainability 2023, Vol. 15, Page 3317*, vol. 15, no. 4, p. 3317, Feb. 2023, doi: 10.3390/SU15043317.
[45] M. C. Kaya, M. S. Nikoo, M. L. Schwartz, and H. Oguztuzun, "Internet of Measurement Things Architecture: Proof of Concept with Scope of Accreditation," *Sensors*, vol. 20, no. 2, p. 503, 2020, doi: 10.3390/s20020503.
[46] R. Hireche, H. Mansouri, and A.-S. K. Pathan, "Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis," *Journal of cybersecurity and privacy*, vol. 2, no. 3, pp. 640–661, 2022, doi: 10.3390/jcp2030033.
[47] K. Thiyagarajan, G. K. Rajini, and D. Maji, "Cost-Effective, Disposable, Flexible, and Printable MWCNT-Based Wearable Sensor for Human Body Temperature Monitoring," *IEEE Sens J*, vol. 22, no. 17, pp. 16756–16763, 2022, doi: 10.1109/jsen.2021.3088466.
[48] F. Wu, T. Wu, and M. R. Yuce, "Design and Implementation of a Wearable Sensor Network System for IoT-Connected Safety and Health Applications," 2019, doi: 10.1109/wf-iot.2019.8767280.
[49] H. Saeed *et al.*, "Blockchain technology in healthcare: A systematic review," *PLoS One*, vol. 17, no. 4, pp. e0266462–e0266462, 2022, doi: 10.1371/journal.pone.0266462.
[50] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control," *J Med Syst*, vol. 40, no. 10, 2016, doi: 10.1007/s10916-016-0574-6.
[51] S. L. T. Vangipuram, S. P. Mohanty, and E. Kougianos, "CoviChain: A Blockchain Based Framework for Nonrepudiable Contact Tracing in Healthcare Cyber-Physical Systems During Pandemic Outbreaks," *SN Comput Sci*, vol. 2, no. 5, 2021, doi: 10.1007/s42979-021-00746-x.
[52] S. H. Alsamhi, B. Lee, and Y. Qiao, "Blockchain for Multi-Robot Collaboration to Combat COVID-19 and Future Pandemics," *IEEE Access*, p. 1, 2020, doi: 10.1109/access.2020.3032450.
[53] A. Al-Meer and S. Al-Kuwari, "Physical Unclonable Functions (PUF) for IoT Devices," *ACM Comput Surv*, 2023, doi: 10.1145/3591464.
[54] M. Codari, S. Schiaffino, F. Sardanelli, and R. M. Trimboli, "Artificial Intelligence for Breast MRI in 2008–2018: A Systematic Mapping Review," *American Journal of Roentgenology*, vol. 212, no. 2, pp. 280–292, 2019, doi: 10.2214/ajr.18.20389.
[55] K. Haseeb, I. Ahmad, I. I. Awan, J. Lloret, and I. Bosch, "A Machine Learning SDN-Enabled Big Data Model for IoMT Systems," *Electronics (Basel)*, vol. 10, no. 18, p. 2228, 2021, doi: 10.3390/electronics10182228.
[56] A. Rahman *et al.*, "Internet of medical things and blockchain-enabled patient-centric agent through SDN for remote patient monitoring in 5G network," *Scientific Reports 2024 14:1*, vol. 14, no. 1, pp. 1–19, Mar. 2024, doi: 10.1038/s41598-024-55662-w.
[57] A. A. Mutlag, Mohd, N. Arunkumar, M. A. Mohammed, and O. Mohd, "Enabling technologies for fog computing in healthcare IoT systems," *Future Generation Computer Systems*, vol. 90, pp. 62–78, 2019, doi: 10.1016/j.future.2018.07.049.
[58] A. Rahman, E. Hassanain, and M. S. Hossain, "Towards a Secure Mobile Edge Computing Framework for Hajj," *IEEE Access*, vol. 5, pp. 11768–11781, 2017, doi: 10.1109/access.2017.2716782.
[59] M. Abdel-Basset, V. Chang, and N. A. Nabeeh, "An intelligent framework using disruptive technologies for COVID-19 analysis," *Technol Forecast Soc Change*, vol. 163, p. 120431, 2021, doi: 10.1016/j.techfore.2020.120431.
[60] Y. Tai, B. Gao, Q. Li, Z. Yu, C. Zhu, and V. Chang, "Trustworthy and Intelligent COVID-19 Diagnostic IoMT Through XR and Deep-Learning-Based Clinic Data Access," *IEEE Internet Things J*, vol. 8, no. 21, pp. 15965–15976, 2021, doi: 10.1109/jiot.2021.3055804.
[61] S. Cheikh Youssef *et al.*, "Evolution of the digital operating room: the place of video technology in surgery," *Langenbecks Arch Surg*, vol. 408, no. 1, Dec. 2023, doi: 10.1007/S00423-023-02830-7.
[62] M. P. Rogers, A. J. DeSantis, H. Janjua, T. M. Barry, and P. C. Kuo, "The future surgical training paradigm: Virtual reality and machine learning in surgical education," *Surgery*, vol. 169, no. 5, pp. 1250–1252, May 2021, doi: 10.1016/J.SURG.2020.09.040.
[63] Y. Khourdifi, A. Elalami, M. Bahaj, M. Zaydi, and O. Er-Remyly, "Framework for integrating healthcare big data using IoMT technology," *Elsevier eBooks*, pp. 191–210, 2023, doi: 10.1016/b978-0-323-99421-7.00012-x.
[64] Y. Khourdifi, A. Elalami, M. Bahaj, M. Zaydi, and O. Er-Remyly, "Framework for integrating healthcare big data using IoMT technology," *Computational Intelligence for Medical Internet of Things (MIoT) Applications*, pp. 191–210, Jan. 2023, doi: 10.1016/B978-0-323-99421-7.00012-X.
[65] S. ; Hamid *et al.*, "A Systematic Review and IoMT Based Big Data Framework for COVID-19 Prevention and Detection," *Electronics 2022, Vol. 11, Page 2777*, vol. 11, no. 17, p. 2777, Sep. 2022, doi: 10.3390/ELECTRONICS11172777.
[66] Y. Wang, L. A. Kung, and T. A. Byrd, "Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations," *Technol Forecast Soc Change*, vol. 126, pp. 3–13, 2018, doi: 10.1016/j.techfore.2015.12.019.
[67] L. Sedov, A. Krasnochub, and V. Polishchuk, "Modeling quarantine during epidemics and mass-testing using drones," *PLoS One*, vol. 15,

no. 6, pp. e0235307–e0235307, 2020, doi: 10.1371/journal.pone.0235307.

[68] Syed, Ain, M. A. Khan, M. H. Alsharif, I. A. Elhaty, and A. Jahid, "Role of Drone Technology Helping in Alleviating the COVID-19 Pandemic," *Micromachines (Basel)*, vol. 13, no. 10, p. 1593, 2022, doi: 10.3390/mi13101593.

[69] Z. Zeng, P.-J. Chen, and A. A. Lew, "From high-touch to high-tech: COVID-19 drives robotics adoption," *Tourism Geographies*, vol. 22, no. 3, pp. 724–734, May 2020, doi: 10.1080/14616688.2020.1762118.

[70] Z. H. Khan, A. Siddique, and C. W. Lee, "Robotics Utilization for Healthcare Digitization in Global COVID-19 Management," *Int J Environ Res Public Health*, vol. 17, no. 11, p. 3819, 2020, doi: 10.3390/ijerph17113819.

[71] M. Podpora, A. Gardecki, R. Beniak, B. Klin, J. L. Vicario, and A. Kawala-Sterniuk, "Human Interaction Smart Subsystem—Extending Speech-Based Human-Robot Interaction Systems with an Implementation of External Smart Sensors," *Sensors*, vol. 20, no. 8, p. 2376, 2020, doi: 10.3390/s20082376.

[72] M. Ghalan and N. Rajesh, "Advancing Human Activity Recognition: A Novel WAECN-BO Approach for Distinguishing Highly Correlated Actions," *Evergreen*, vol. 10, no. 4, pp. 2398–2411, 2023, doi: 10.5109/7160930.

[73] R. Alizadehsani *et al.*, "Swarm Intelligence in Internet of Medical Things: A Review," *Sensors*, vol. 23, no. 3, p. 1466, 2023, doi: 10.3390/s23031466.

[74] L. Falaschetti, M. Alessandrini, G. Biagetti, P. Crippa, and C. Turchetti, "ECG-Based Arrhythmia Classification using Recurrent Neural Networks in Embedded Systems," *Procedia Comput Sci*, vol. 207, pp. 3479–3487, 2022, doi: 10.1016/j.procs.2022.09.406.

[75] Q. Qu, H. Sun, and Y. Chen, "Smart Healthcare at Home in the Era of IoMT," *IntechOpen eBooks*, 2023, doi: 10.5772/intechopen.113208.

[76] M. F. Khan *et al.*, "An IoMT-Enabled Smart Healthcare Model to Monitor Elderly People Using Machine Learning Technique," *Comput Intell Neurosci*, vol. 2021, pp. 1–10, 2021, doi: 10.1155/2021/2487759.

[77] B. R. Barricelli, E. Casiraghi, and D. Fogli, "A Survey on Digital Twin: Definitions, Characteristics, Applications, and Design Implications," *IEEE Access*, vol. 7, pp. 167653–167671, 2019, doi: 10.1109/access.2019.2953499.

[78] Y. Liu *et al.*, "A Novel Cloud-Based Framework for the Elderly Healthcare Services Using Digital Twin," *IEEE Access*, vol. 7, pp. 49088–49101, 2019, doi: 10.1109/access.2019.2909828.

[79] M. M. Madine *et al.*, "Blockchain for Giving Patients Control Over Their Medical Records," *IEEE Access*, vol. 8, pp. 193102–193115, 2020, doi: 10.1109/access.2020.3032553.

[80] Y. J. Fan, Y. H. Yin, L. Da Xu, Y. Zeng, and F. Wu, "IoT-Based Smart Rehabilitation System," *IEEE Trans Industr Inform*, vol. 10, no. 2, pp. 1568–1577, 2014, doi: 10.1109/tii.2014.2302583.

[81] N. Shoaip, A. Rezk, S. El-Sappagh, L. Alarabi, S. Barakat, and M. M. Elmogy, "A Comprehensive Fuzzy Ontology-Based Decision Support System for Alzheimer's Disease Diagnosis," *IEEE Access*, vol. 9, pp. 31350–31372, 2021, doi: 10.1109/access.2020.3048435.

[82] P. Ramesh, J. M. Sahayaraj, N. Subash, S. R. Mugunthan, and S. J. Pratha, "IoT based Waste Management System," *2022 International Conference on Electronics and Renewable Systems (ICEARS)*, 2022, doi: 10.1109/icears53579.2022.9752091.

[83] S. Tripathi *et al.*, "IoMT-Enabled Smart Healthcare: State-of-the-Art, Security and Future Directions," 2023, doi: 10.1109/ikt62039.2023.10433013.

[84] Z. Ashfaq *et al.*, "A review of enabling technologies for Internet of Medical Things (IoMT) Ecosystem," *Ain Shams Engineering Journal*, vol. 13, no. 4, p. 101660, 2022, doi: 10.1016/j.asej.2021.101660.

[85] L. P. Malasinghe, N. Ramzan, and K. P. Dahal, "Remote patient monitoring: a comprehensive study," *J Ambient Intell Humaniz Comput*, vol. 10, no. 1, pp. 57–76, 2017, doi: 10.1007/s12652-017-0598-x.

[86] T. Battelino *et al.*, "Continuous glucose monitoring and metrics for clinical trials: an international consensus statement," *Lancet Diabetes Endocrinol*, vol. 11, no. 1, pp. 42–57, 2023, doi: 10.1016/s2213-8587(22)00319-9.

[87] S. Bhatta, "Empowering Rural Healthcare: MobileNet-Driven Deep Learning for Early Diabetic Retinopathy Detection in Nepal," *Journal of Electronics, Electromedical Engineering, and Medical Informatics*, vol. 5, no. 4, pp. 290–302, Oct. 2023, doi: 10.35882/JEEEMI.V5I4.326.

[88] M. Matthews, S. Abdullah, G. Gay, and T. Choudhury, "Tracking Mental Well-Being: Balancing Rich Sensing and Patient Needs," *IEEE Computer*, vol. 47, no. 4, pp. 36–43, 2014, doi: 10.1109/mc.2014.107.

[89] A. Mamun, M. A. Alhussein, K. Sailunaz, and M. S. Islam, "Cloud-based framework for Parkinson's disease diagnosis and monitoring system for remote healthcare applications," *Future Generation Computer Systems*, vol. 66, pp. 36–47, 2017, doi: 10.1016/j.future.2015.11.010.

[90] L. Catarinucci *et al.*, "An IoT-Aware Architecture for Smart Healthcare Systems," *IEEE Internet Things J*, vol. 2, no. 6, pp. 515–526, 2015, doi: 10.1109/jiot.2015.2417684.

[91] R. Islam, D. Kwak, Md. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," *IEEE Access*, vol. 3, pp. 678–708, 2015, doi: 10.1109/access.2015.2437951.

[92] S. B. Baker, W. Xiang, and I. Atkinson, "Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities," *IEEE Access*, vol. 5, pp. 26521–26544, 2017, doi: 10.1109/access.2017.2775180.

[93] D. Dziak, B. Jachimczyk, and W. Kulesza, "IoT-Based Information System for Healthcare Application: Design Methodology Approach," *Applied Sciences*, vol. 7, no. 6, p. 596, 2017, doi: 10.3390/app7060596.

[94] F. Jiang, Y. Jiang, and H. Zhi, "Artificial intelligence in healthcare: past, present and future," *Stroke Vasc Neurol*, vol. 2, no. 4, pp. 230–243, 2017, doi: 10.1136/svn-2017-000101.

[95] L. Pantanowitz *et al.*, "An artificial intelligence algorithm for prostate cancer diagnosis in whole slide images of core needle biopsies: a blinded clinical validation and deployment study," *Lancet Digit Health*, vol. 2, no. 8, pp. e407–e416, 2020, doi: 10.1016/s2589-7500(20)30159-x.

[96] S. P. Somashekhar, R. Kumar, A. Rauthan, K. R. Arun, P. Patil, and Y. E. Ramya, "Abstract S6-07: Double-blinded validation study to assess performance of IBM artificial intelligence platform, Watson for oncology in comparison with Manipal multidisciplinary tumor board – First study of 638 breast cancer cases," *General Session Abstracts*, 2017, doi: 10.1158/1538-7445.sabcs16-s6-07.

[97] A. Esteva *et al.*, "Dermatologist-level classification of skin cancer with deep neural networks," *Nature*, vol. 542, no. 7639, pp. 115–118, 2017, doi: 10.1038/nature21056.

[98] C. E. Bouton *et al.*, "Restoring cortical control of functional movement in a human with quadriplegia," *Nature*, vol. 533, no. 7602, pp. 247–250, 2016, doi: 10.1038/nature17435.

[99] S. Jha and E. J. Topol, "Adapting to Artificial Intelligence," *JAMA*, vol. 316, no. 22, p. 2353, 2016, doi: 10.1001/jama.2016.17438.

[100] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, "Security in IoMT Communications: A Survey," *Sensors (Basel)*, vol. 20, no. 17, pp. 1–49, Sep. 2020, doi: 10.3390/S20174828.

[101] A. Lazaro, R. Villarino, M. Lazaro, N. Canellas, B. Prieto-Simon, and D. Girbau, "Recent Advances in Batteryless NFC Sensors for Chemical Sensing and Biosensing," *Biosensors (Basel)*, vol. 13, no. 8, Aug. 2023, doi: 10.3390/BIOS13080775.

[102] C. S. Chang, T. H. Wu, Y. C. Wu, and C. C. Han, "Bluetooth-Based Healthcare Information and Medical Resource Management System," *Sensors (Basel)*, vol. 23, no. 12, Jun. 2023, doi: 10.3390/S23125389.

[103] R. Sastry, B. Ch, and R. R. Budaraju, "Implementing Dual Base Stations within an IoT Network for Sustaining the Fault Tolerance of an IoT Network through an Efficient Path Finding Algorithm," *Sensors*, vol. 23, no. 8, p. 4032, 2023, doi: 10.3390/s23084032.

[104] H. Ge, L. Li, D. Zhang, and F. Ma, "Applications of digital Medicine in oncology: Prospects and challenges," *Cancer Innovation*, vol. 1, no. 4, pp. 285–292, 2022, doi: 10.1002/cai2.37.

[105] S. A. Ajagbe, J. B. Awotunde, A. O. Adesina, P. Achimugu, and T. A. Kumar, "Internet of Medical Things (IoMT): Applications, Challenges, and Prospects in a Data-Driven Technology," pp. 299–319, 2022, doi: 10.1007/978-981-16-8150-9_14.

[106] D. Jain, "Regulation of Digital Healthcare in India: Ethical and Legal Challenges," *Healthcare*, vol. 11, no. 6, Mar. 2023, doi: 10.3390/HEALTHCARE11060911.
[107] B. Varkey, "Principles of Clinical Ethics and Their Application to Practice," *Medical Principles and Practice*, vol. 30, no. 1, pp. 17–28, 2020, doi: 10.1159/000509119.

AUTHORS BIOGRAPHY

Ms Manishka Mukhopadhyay is a Bachelor of Technology in Industrial and Systems Engineering from the Indian Institute of Technology, Kharagpur, India. Her micro specialization is in Artificial intelligence. She has done her research work on self-supervised learning algorithms for implementation in Industrial IoT. Earlier she had also worked at Deakin University where she developed zero-shot learning algorithms for autonomous vehicles. She has worked at the Centre of Excellence of Advanced Manufacturing Technique at IIT, Kharagpur to develop to apply Industry 4.0 in production and manufacturing.

Mr.Subhrajyoti Banerjee obtained his MSc in Biotechnology (2018) from West Bengal University of Technology (now MAKAUT) and then did his MSc (2020) in Biotechnology from Techno India University (TIU). He worked at the Department of Biotechnology, Techno India University as a teaching aid for 2 years (2020-2022) and joined the Indian Institute of Engineering Science and Technology (IIEST) for MTech in Biomedical Engineering. He is now in the final semester of his PG course. His research interest is to identify biomarkers for early diagnosis of brain malignancy. He is working on the importance of liquid biopsy for early brain cancer detection.

Dr. Chitrangada Das Mukhopadhyay did her Mtech in Biotechnology and Engineering from the Indian Institute of Technology and then did her PhD from the same Institute. Then she did her postdoctoral research at Ohio State University Medical Centre and finally joined the Indian Institute of Engineering Science and Technology as a faculty of the Centre for Healthcare Science and Technology. Her research area is to develop novel therapeutics for malignant brain tumors and neurodegenerative diseases, using Functional genomics, Bioinformatics, and drug design techniques. Students at this lab have developed electromagnetic devices to treat glioblastoma by creating gentle and focused hyperthermia and to treat Alzheimer's' disease by reestablishing Ca homeostasis.