Engineering and Technology Journal e-ISSN: 2456-3358
Volume 10 Issue 08 August-2025, Page No.-6321-6334
DOI: 10.47191/etj/v10i08.26, I.F. – 8.482

The Internet of Medical Things (IoMT): A Comprehensive Review of Architecture, Enabling Technologies, Security Challenges, And Future Perspectives

Jackson Muketo Mutua[1], Hilda Jemutai Bitok[2]
[1]Department of Information Technology and Informatics (ITI), School of Computing and Information Technology (SCIT) & Kaimosi Friends University, Kaimosi, Kenya.
[2]School of Science, Technology and Engineering, University of the Sunshine Coast, Queensland Australia

ABSTRACT: The Internet of Medical Things (IoMT) integrates interconnected medical devices, sensors, and systems to collect and analyze health data via internet-based technologies. This ecosystem includes wearables, implantable sensors, and hospital equipment, enabling real-time data acquisition for enhanced clinical decisions, cost reduction, and improved patient outcomes. IoMT supports applications like telemedicine, remote monitoring, and personalized treatment, addressing needs in aging populations and underserved regions.

This study examines IoMT's architecture, comprising device, network, and cloud layers, emphasizing interoperability with healthcare systems. Enabling technologies like 5G, edge computing, AI, and blockchain enhance data transmission and security. However, IoMT faces significant security challenges, including data breaches and unauthorized access, necessitating robust encryption, authentication, and compliance with standards like HIPAA and GDPR. Future directions include AI-driven analytics, personalized medicine, and scalable healthcare models. Despite its potential, issues like privacy, interoperability, and cybersecurity must be addressed for sustainable implementation. This review provides a holistic understanding of IoMT, highlighting its transformative role in smart healthcare and offering insights into its challenges and opportunities.

KEYWORDS: Internet of Medical Things (IoMT), Interoperability, Telemedicine, Cybersecurity, AI-driven analytics

1. INTRODUCTION

The Internet of Things (IoT) paradigm revolutionizes connectivity by enabling seamless communication among physical objects, such as sensors, actuators, and electronic devices, across various sectors, including smart cities, transportation, and healthcare [1]. Within this expansive framework, the Internet of Medical Things (IoMT) emerges as a transformative application of IoT principles tailored specifically to the healthcare domain. IoMT facilitates the collection, transmission, and analysis of health-related data through interconnected medical devices and systems linked via the internet [2]. This ecosystem encompasses a diverse array of devices, from wearable health monitors like fitness trackers and smartwatches to implantable sensors and sophisticated hospital equipment, such as advanced imaging systems and patient monitoring tools [3]. These devices operate autonomously, requiring minimal human intervention, and enable real-time health monitoring, diagnostics, and data-driven decision-making. By providing healthcare professionals with actionable insights, IoMT enhances clinical workflows, optimizes resource allocation, and delivers value-based care, ultimately improving patient outcomes and quality of life [4].

The rapid adoption of IoMT has been driven by an increasing demand for remote healthcare solutions, a need amplified by global health challenges like the COVID-19 pandemic [5]. The crisis underscored the importance of telemedicine, virtual consultations, and remote patient monitoring, which allowed healthcare providers to monitor vital signs, symptoms, and health metrics without necessitating in-person visits. This shift significantly reduced the risk of disease transmission while addressing the growing burden of chronic conditions, such as diabetes, hypertension, and cardiovascular diseases, which have become more prevalent worldwide. For example, according to the Fortune Business insights, the IoMT market has seen remarkable growth, with its value in North America reaching USD 41.17 billion in 2020 and projected to surge by 660% from USD 48.7 billion in 2022 to USD 370.9 billion by 2032[6]. This exponential expansion reflects the increasing reliance on IoMT to deliver accessible, efficient, and scalable healthcare solutions, particularly in underserved regions and for aging populations [6].

Technological advancements underpin IoMT's transformative potential. Innovations such as 5G connectivity enable rapid and reliable data transmission, while edge computing supports real-time data processing at the source, reducing latency and enhancing efficiency [7]. Artificial intelligence (AI) plays a pivotal role by powering predictive analytics, enabling early detection of health issues, and personalizing treatment plans based on individual patient data. Blockchain technology strengthens data security, ensuring the integrity and confidentiality of sensitive health information. Additionally, emerging technologies like Bio-Nano Things—miniature devices operating at the molecular level—promise to further revolutionize diagnostics and treatment delivery [8]. These advancements collectively enhance the scalability, reliability, and precision of IoMT systems, paving the way for smarter healthcare ecosystems.

Regulatory frameworks, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union, play a critical role in shaping IoMT’s development [9]. These regulations enforce stringent standards for data security and patient privacy, ensuring that IoMT solutions are both dependable and compliant. Robust encryption, secure authentication mechanisms, and adherence to these standards safeguard sensitive health data against breaches and unauthorized access, fostering trust among patients and providers. However, challenges such as interoperability between diverse IoMT devices, cybersecurity threats, and the complexity of integrating new technologies with existing healthcare infrastructures must be addressed to fully realize IoMT’s potential [10].

Looking ahead, IoMT is poised to redefine healthcare delivery by fostering proactive, patient-centric care models. Wearable devices and remote monitoring tools empower patients to actively manage their health, while AI-driven analytics enable early intervention and tailored therapies [11]. The integration of IoMT into personalized medicine holds promise for more precise and effective treatments, particularly for chronic and complex conditions [12]. As healthcare demands continue to evolve, IoMT’s ability to provide accessible, efficient, and scalable solutions positions it as a cornerstone of modern healthcare. By overcoming challenges like data privacy, system interoperability, and regulatory compliance, IoMT will drive the transition toward smarter, more inclusive healthcare systems, transforming the way care is delivered worldwide.

2. LITERATURE REVIEW

2.1 Architecture of IoMT

The Internet of Medical Things (IoMT) architecture comprises interconnected layers that enable seamless collection, transmission, processing, and utilization of health data [13]. Each layer plays a critical role in ensuring efficient, secure, and scalable healthcare delivery. Below is an in-depth exploration of the IoMT architectural framework, expanding on its core components to provide a comprehensive understanding of its functionality and significance.

2.1.1 Device Layer

The device layer forms the foundation of the IoMT ecosystem, encompassing a diverse array of medical devices designed to capture and transmit health-related data [14]. These devices are equipped with advanced sensors to monitor vital signs and other physiological parameters in real time, enabling continuous health tracking without human intervention. Key components include:

Wearable Devices: Devices such as smartwatches, fitness trackers, and biosensors worn on the body monitor metrics like heart rate, blood oxygen levels, sleep patterns, and physical activity [15]. For instance, smartwatches can track irregular heart rhythms, alerting users to potential cardiac issues.

Implantable Devices: These include pacemakers, insulin pumps, and neurostimulators embedded within the body to manage chronic conditions [16]. For example, continuous glucose monitors (CGMs) provide real-time blood sugar readings for diabetic patients, enabling timely interventions.

Stationary Devices: Hospital-based equipment, such as electrocardiogram (ECG) machines, magnetic resonance imaging (MRI) systems, and patient monitors, collect high-fidelity data for diagnostics and treatment planning [17]. These devices are increasingly integrated with IoMT networks for seamless data sharing.

Sensors embedded in these devices, such as temperature, pressure, and biochemical sensors, ensure precise and continuous data collection. This layer’s ability to generate actionable health data is pivotal for enabling proactive care and supporting remote monitoring, particularly for patients in underserved or remote areas.

2.1.2 Connectivity Layer

The connectivity layer serves as the backbone of IoMT, facilitating secure and reliable communication between devices, local networks, and cloud systems [18]. This layer ensures that data collected from the device layer is transmitted efficiently for processing and analysis. Its key components include:

Communication Protocols: IoMT relies on a variety of protocols to enable device connectivity, including Bluetooth Low Energy (BLE) for short-range, low-power communication, Wi-Fi for high-speed data transfer, Zigbee for low-cost mesh networking, and cellular networks (e.g., 4G/5G) for long-range, high-bandwidth connectivity [19]. The advent of 5G enhances IoMT by offering ultra-low latency and high reliability, critical for real-time applications like telesurgery.

•**Gateways:** Gateways act as intermediaries, aggregating data from multiple IoMT devices and ensuring secure transmission to cloud or local servers. These devices, such as IoT hubs or routers, perform preliminary data filtering and protocol translation to ensure compatibility across heterogeneous devices [20]. For example, a hospital gateway may collect data from bedside monitors and transmit it to a central server for analysis.

This layer's robustness is essential for maintaining uninterrupted data flow, especially in scenarios requiring real-time monitoring, such as critical care or emergency response.

2.1.3 Data Processing Layer

The data processing layer is responsible for transforming raw health data into meaningful insights through computational techniques. It operates at two levels to optimize efficiency and reduce latency:

Edge Computing: Edge computing processes data locally, near the source device, to minimize latency and reduce bandwidth demands [21]. For instance, a wearable device monitoring heart rate may use edge computing to detect anomalies and issue immediate alerts without relying on cloud connectivity [4]. This is particularly valuable in time-sensitive applications, such as detecting seizures or cardiac arrhythmias.

Cloud Computing: For large-scale data storage, analysis, and long-term processing, data is transmitted to cloud servers. Cloud platforms leverage advanced computational resources to perform complex tasks, such as machine learning model training, population health analytics, and trend identification [22]. For example, cloud-based AI algorithms can analyze longitudinal patient data to predict disease progression or optimize treatment plans.

The synergy between edge and cloud computing ensures that IoMT systems balance real-time responsiveness with comprehensive data analysis, enabling both immediate interventions and strategic healthcare planning.

2.1.4. Application Layer

The application layer translates processed data into actionable healthcare solutions, delivering value to patients, providers, and healthcare systems. This layer encompasses software and platforms that facilitate clinical and patient-facing functionalities:

Healthcare Applications: These include telemedicine platforms for virtual consultations, remote patient monitoring systems for continuous health tracking, and health analytics tools for deriving insights. For example, a telemedicine app may enable a doctor to review a patient's vital signs in real time during a virtual visit, improving access to care for rural or mobility-constrained patients [23].

Data Analytics: Advanced analytics tools, powered by AI and machine learning, process large datasets to identify patterns, predict health risks, and support personalized treatment plans. Predictive analytics can forecast potential complications, such as heart failure in at-risk patients, enabling early interventions. Additionally, population health analytics can guide public health strategies by identifying disease trends across communities [23].

This layer bridges the gap between raw data and practical healthcare solutions, fostering proactive care models and improving patient engagement.

2.1.5 User Interface Layer

The user interface layer provides accessible and intuitive platforms for stakeholders to interact with IoMT systems, ensuring that health data is meaningful and actionable for both patients and providers:

Patient Interfaces: Mobile apps and web portals empower patients to monitor their health metrics, receive real-time alerts, and communicate with healthcare providers. For example, a diabetes management app may display glucose trends, recommend insulin adjustments, and send reminders for medication adherence, enhancing patient autonomy and engagement [24].

Provider Interfaces: Dashboards and clinical decision support systems enable healthcare professionals to access comprehensive patient data, monitor trends, and make informed decisions. For instance, a hospital dashboard may display real-time vitals from multiple patients, allowing clinicians to prioritize critical cases and streamline workflows [25].

These interfaces are designed with user-centric principles, ensuring ease of use, accessibility, and compatibility with diverse devices, such as smartphones, tablets, and desktops.

2.1.6. Security Layer

Given the sensitive nature of health data, the security layer is critical to protecting patient privacy and ensuring system integrity. This layer encompasses mechanisms to safeguard data across all IoMT layers:

Data Security: Robust encryption protocols, such as AES-256, secure data during transmission and storage. Authentication mechanisms, including multi-factor authentication (MFA) and biometric verification, prevent unauthorized access. Access control policies ensure that only authorized personnel can view or modify sensitive data, reducing the risk of breaches [26].

Compliance: IoMT systems must adhere to stringent regulatory standards, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union. Compliance involves implementing secure data handling practices, conducting regular audits, and ensuring transparency in data usage to maintain patient trust [27].

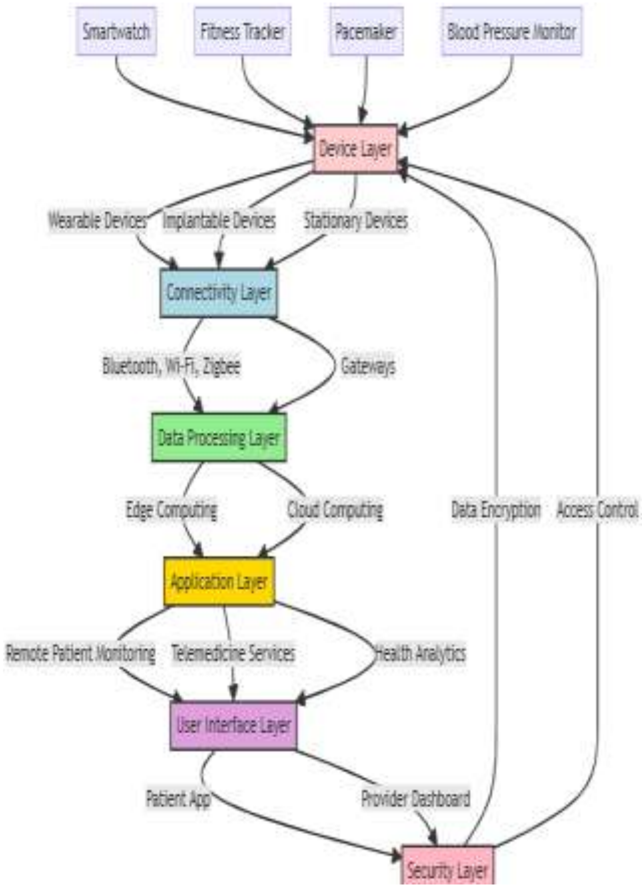

Figure 1: IoMT Architecture

2.2 IoMT ENABLING TECHNOLOGIES

In this section, we will explore the enabling technologies that underpin each layer of the Internet of Medical Things (IoMT). These technologies are essential for facilitating communication, data management, and integration within the healthcare ecosystem.

2.2.1 Enabling Technologies for Device Layer in IoMT

There are several important enabling technologies for device layer of the IoMT architecture. These technologies are essential for gathering physiological data, environmental data, and vital signs. Some of these technologies are:

Biosensors: Biosensors detect and measure biological or chemical data from the body by converting biological signals into electrical impulses for further processing and analysis [28] They can measure variables such as blood pressure, oxygen saturation, blood glucose levels, and heart rate. Examples include electrocardiogram (ECG) sensors, glucose sensors, and pulse oximeters, which play a vital role in monitoring physiological activities and identifying indicators for diagnosing and managing diseases [29].

Wearable Devices: Wearable technologies, such as smartwatches, fitness trackers, and patches, incorporate sensors that continuously track physiological indicators [30]. These devices monitor parameters like heart rate, activity levels, sleep patterns, body temperature, and electrodermal activity. Modern smart glasses, equipped with sensors like gyroscopes and accelerometers, can be viewed as wearable computers, often connected to cloud-based applications for real-time data analysis and visualization [31].

Implantable Sensors: Implantable sensors are miniature devices placed inside the body to continuously monitor specific health metrics. They are used for applications such as measuring intraocular pressure in glaucoma patients, monitoring glucose levels in diabetics, and tracking cardiac activity in patients with heart issues. These sensors provide long-term monitoring and can wirelessly transmit data to healthcare professionals [32].

Ingestible Sensors: Ingestible sensors are small, wireless devices that can be swallowed in the form of pills or capsules. They include pH sensors, temperature sensors, pressure sensors, and biochemical sensors designed to withstand the digestive system. Once ingested, they collect data on pH values, temperature changes, or gastrointestinal biomarkers and wirelessly transmit this information to external devices, offering a non-invasive alternative to traditional diagnostic methods [33].

Environmental Sensors: Environmental sensors continuously monitor physical phenomena that can affect health or well-being, such as temperature, humidity, air quality, noise levels, and radiation. These sensors are installed in homes, hospitals, or public spaces to assess environmental quality and provide early warnings about potential health hazards [34].

Motion Sensors: Motion sensors, including accelerometers and gyroscopes, are commonly used in IoMT applications to record movement and activity data. They can monitor physical activity levels, detect falls or abnormal movement patterns, and provide insights into a patient's mobility and recovery. These sensors are often integrated into wearable technologies or placed in the environment [35].

Imaging Technologies: Imaging techniques such as X-rays, ultrasounds, magnetic resonance imaging (MRI), and computed tomography (CT) are essential for obtaining detailed visual data about internal body structures. These technologies aid in disease monitoring, diagnosis, and treatment planning, and imaging data can be integrated with other IoMT components for a comprehensive view of patient health [36].

Remote Monitoring Devices: Remote monitoring devices utilize various sensors and technologies for continuous health parameter monitoring over long distances. They reduce the need for frequent hospital visits by allowing healthcare professionals to monitor patients in their homes or non-clinical settings. These devices can assess factors such as heart rate, blood pressure, oxygen saturation, respiration rate, and temperature [37].

Biometric Identification: Biometric sensors in the IoMT paradigm are used for authentication and identification purposes. They collect biometric data such as fingerprints, iris patterns, voiceprints, or facial recognition to ensure secure access to medical devices and patient data. This technology helps mitigate the risk of unauthorized access and data breaches [38].

Smart Textiles: Smart textiles incorporate sensors and conductive materials into fabrics to monitor physiological parameters. These textiles can measure heart rate, respiration rate, and body temperature while being worn as clothing. They provide a comfortable and non-intrusive way to collect health data, making them ideal for continuous monitoring in various settings, including sports and rehabilitation [39].

2.2.2 Enabling Technologies in the Connectivity Layer of IoMT

Wireless Communication Protocols

Bluetooth: Bluetooth is a short-range wireless communication technology that enables devices to connect and communicate over distances typically up to 100 meters. It is commonly used in wearables (like fitness trackers and smartwatches) to transmit health data (e.g., heart rate, activity levels) to smartphones or computers. Bluetooth Low Energy (BLE) is particularly favored for its low power consumption, making it ideal for battery-operated devices [40].

Wi-Fi: Wi-Fi provides high-speed internet access and allows devices to connect to local networks and the internet. In healthcare settings, Wi-Fi supports real-time data transfer from medical devices to servers or cloud platforms, enabling remote monitoring and telehealth services. It is essential for devices that require large data uploads, such as imaging equipment [9].

Zigbee: Zigbee is a low-power, low-data-rate wireless protocol designed for short-range communication, typically within a range of 10-100 meters. It is suitable for sensor networks in medical environments, such as patient monitoring systems, where multiple devices need to communicate with a central hub. Its low power consumption extends battery life for devices like wearable sensors [41].

LoRaWAN (Long Range Wide Area Network): LoRaWAN is designed for long-range communication with low power requirements, making it ideal for IoMT applications. It is particularly useful for remote health monitoring, allowing sensors to transmit data over several kilometres without needing a constant power source. This is beneficial for monitoring patients in rural areas or those with mobility issues [7].

Cellular Networks

4G LTE and 5G:4G LTE provides high-speed mobile internet, while 5G offers even faster speeds and lower latency. These networks enable real-time communication for mobile health applications, such as telemedicine and remote patient monitoring. 5G, with its enhanced capabilities, supports high-definition video consultations and the use of advanced applications like augmented reality in healthcare [19].

NB-IoT (Narrowband IoT): NB-IoT is a cellular technology specifically designed for IoT devices that require low power consumption and long-range connectivity. It is ideal for applications like remote monitoring of chronic patients, where devices need to send small amounts of data infrequently. This technology allows for extensive coverage in urban and rural settings [36].

Satellite Communication: Satellite communication provides connectivity in areas where traditional communication infrastructure (like cellular or Wi-Fi) is not available [28]. It is particularly valuable for telemedicine in remote or underserved regions, enabling healthcare providers to monitor patients and share data regardless of geographical barriers [42].

Middleware Solutions: Middleware acts as a bridge between different software applications, facilitating data exchange and integration. In the IoMT ecosystem, middleware solutions enable interoperability among various medical devices, applications, and databases, streamlining workflows and enhancing data accessibility for healthcare providers [43].

Application Programming Interfaces (APIs): APIs are sets of rules and protocols that allow different software applications to communicate with each other. APIs enable seamless integration of IoMT devices with electronic health records (EHRs) and other healthcare systems, allowing for efficient data sharing and improved patient management [20].

Cloud Computing: Cloud computing provides scalable storage and processing capabilities over the internet. Cloud platforms allow healthcare providers to store and analyze vast amounts of data collected from IoMT devices. This enables remote access to patient information, supports collaborative care models, and facilitates data analytics for better decision-making [22].

Edge Computing

Edge computing processes data closer to the source (e.g., on the device or local server) rather than relying solely on centralized cloud servers. This technology reduces latency and bandwidth usage, which is critical for applications requiring real-time responses, such as alert systems for abnormal vital signs or immediate feedback during surgeries [26].

2.3 Enabling Technologies in the Data Processing Layer of IoMT

Data Analytics Tools: Data analytics tools are crucial in this layer, as they are designed to analyze and interpret large datasets using various statistical and computational techniques. These tools extract valuable insights from patient data collected from wearables, biosensors, and other medical devices [44]. For instance, predictive analytics can identify trends in patient health metrics, allowing healthcare providers to intervene proactively before complications arise. Tools such as Tableau, Power BI, and specialized healthcare analytics platforms enable visualization and reporting of health data, making it easier for clinicians to understand complex information [18].

Machine Learning and Artificial Intelligence (AI): Machine learning (ML) and artificial intelligence (AI) play a transformative role in data processing within IoMT. These technologies involve algorithms that learn from data to make predictions or decisions without explicit programming [18]. In healthcare, AI and ML can analyze complex health data to identify patterns and predict outcomes. For example, algorithms can be developed to predict the likelihood of hospital readmissions based on patient history and real-time monitoring data. Additionally, AI-powered systems can assist in diagnostic imaging by identifying anomalies in X-rays or MRIs faster and more accurately than human radiologists [24].

Big Data Technologies: Big data technologies are integral to the data processing layer, as they provide the tools and frameworks necessary to handle and process massive volumes of data that traditional systems cannot manage effectively [16]. Platforms like Apache Hadoop and Apache Spark enable the storage and processing of large datasets generated by IoMT devices. These technologies allow for distributed data processing, making it possible to analyze vast amounts of health data quickly and efficiently. This capability is crucial for aggregating data from multiple sources, including electronic health records (EHRs), wearables, and clinical trials [44].

Cloud Computing: Cloud computing offers scalable and flexible computing resources over the internet, allowing for data storage, processing, and management without the need for on-premises infrastructure. In the context of IoMT, cloud services enable healthcare organizations to store and analyze large datasets securely. Major cloud platforms like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud provide tools for data analytics, machine learning, and application development, facilitating collaboration among healthcare providers and researchers [17].

Data Integration and Interoperability Solutions: Data integration and interoperability solutions are vital for consolidating patient data from various devices, applications, and EHR systems. These solutions ensure that different systems can communicate and share data effectively, enabling a unified view of patient information. Standards like HL7 and FHIR (Fast Healthcare Interoperability Resources) facilitate the exchange of health information across different platforms, allowing healthcare providers to access comprehensive patient profiles for better decision-making [22].

Real-Time Data Processing Systems: Real-time data processing systems are designed to analyze data as it is generated, allowing for immediate insights and actions. This capability is essential for applications that require timely responses, such as monitoring vital signs in critical care settings. Technologies like Apache Kafka and Stream Processing frameworks enable the ingestion and analysis of data streams from IoMT devices in real time, allowing for alerts and notifications to healthcare providers when abnormal values are detected [30].

Data Storage Solutions: Data storage solutions encompass various technologies for securely and efficiently storing structured and unstructured data. Relational databases (e.g., MySQL, PostgreSQL) and NoSQL databases (e.g., MongoDB, Cassandra) are commonly used to store patient data collected from IoMT devices. Cloud storage options provide scalable solutions for managing large volumes of health data, ensuring data integrity and availability for analysis [17].

Data Privacy and Security Technologies: Data privacy and security technologies are critical for protecting sensitive health data from unauthorized access and breaches, ensuring compliance with regulations such as HIPAA. Encryption technologies, access controls, and secure data transmission protocols (like HTTPS and TLS) are implemented to safeguard patient information. Additionally, data anonymization techniques are employed to protect patient identity while allowing for data analysis and research [26].

Blockchain Technology: Blockchain technology is emerging as an innovative solution in the data processing layer. This decentralized ledger technology provides secure, transparent, and tamper-proof record-keeping. In the context of IoMT, blockchain can enhance data security and integrity by offering a secure way to store and share patient data across different stakeholders. It can also facilitate secure consent management, ensuring that patients have control over who accesses their health information [38].

2.4 Enabling Technologies in the Application Layer of IoMT

The application layer of IoMT is where software applications interact with the data processed in the lower layers to deliver services and functionalities that improve patient care, enhance operational efficiency, and facilitate communication among stakeholders. Here are the key enabling technologies in this layer:

Mobile Health (mHealth) Applications: Mobile health applications are software solutions designed for smartphones and tablets that enable patients and healthcare providers to monitor health conditions, manage medications, and communicate effectively [23]. These apps can track vital signs, provide reminders for medication, and offer telehealth services, allowing for remote consultations and follow-ups. They empower patients to take an active role in their health management.

Telemedicine Platforms: Telemedicine platforms facilitate remote healthcare delivery through video conferencing, chat, and other communication tools [6]. These platforms enable healthcare providers to conduct virtual consultations, diagnose conditions, and provide treatment recommendations without requiring patients to visit a healthcare facility. This technology increases access to care, especially for patients in remote or underserved areas.

Remote Patient Monitoring (RPM) Systems: Remote patient monitoring systems use connected devices to collect patient data outside of traditional clinical settings. These systems continuously monitor health metrics such as heart rate, blood pressure, and glucose levels, transmitting the data to healthcare providers in real time [20]. This enables proactive management of chronic conditions and timely interventions when abnormalities are detected.

Clinical Decision Support Systems (CDSS): Clinical decision support systems assist healthcare providers in making informed clinical decisions by analyzing patient data and providing evidence-based recommendations. These systems integrate with electronic health records (EHRs) and utilize algorithms to alert clinicians about potential issues, such as drug interactions or deviations from clinical guidelines. CDSS improves patient safety and enhances the quality of care [44].

Health Information Exchange (HIE) Systems: Health information exchange systems enable the secure sharing of patient data across different healthcare organizations and systems. These platforms facilitate interoperability, allowing healthcare providers to access comprehensive patient information, regardless of where the data was generated. HIE systems improve care coordination and ensure that providers have the necessary information for informed decision-making [45].

Electronic Health Records (EHR) Systems: Electronic health records are digital versions of patients' paper charts, consolidating health information in a single, accessible format. EHR systems store a wide range of patient data, including medical history, medications, allergies, and test results. They enhance the efficiency of healthcare delivery, streamline workflows, and improve communication among healthcare providers [39].

Artificial Intelligence (AI) in Healthcare Applications: AI technologies are increasingly being integrated into healthcare applications to enhance diagnostic accuracy, personalize treatment plans, and improve patient engagement. AI algorithms can analyze large datasets to identify patterns, predict outcomes, and assist in clinical decision-making. Applications include image recognition for radiology, natural language processing for clinical documentation, and chatbots for patient interaction [24].

Wearable Health Devices: Wearable health devices, such as smartwatches and fitness trackers, collect health-related data from users in real time. These devices monitor various metrics, including heart rate, physical activity, sleep patterns, and more. The data collected can be shared with healthcare providers to support remote monitoring and personalized health recommendations [39].

Blockchain for Health Data Management: Blockchain technology is being explored in the application layer to enhance the security and integrity of health data management. By providing a decentralized and tamper-proof ledger, blockchain can facilitate secure sharing of patient information among healthcare providers, ensuring data privacy and enhancing trust in health data transactions [19].

Patient Engagement Platforms: Patient engagement platforms aim to enhance communication between patients and healthcare providers. These platforms provide tools for appointment scheduling, health education, and personalized health information. By fostering engagement, these technologies empower patients to take control of their health and improve adherence to treatment plans [4].

2.5 Enabling Technologies in the User Interface Layer of IoMT

The user interface (UI) layer of the Internet of Medical Things (IoMT) is crucial for ensuring that healthcare providers, patients, and other stakeholders can effectively interact with IoMT applications and devices. This layer focuses on the design and functionality of interfaces that facilitate communication, data visualization, and user engagement. Here are the key enabling technologies in this layer:

Web and Mobile Interfaces: Web and mobile interfaces are essential for providing users with access to IoMT applications through browsers or dedicated apps on smartphones and tablets. These interfaces are designed to be intuitive and user-friendly, allowing patients and healthcare providers to easily navigate through features such as health monitoring, appointment scheduling, and telehealth services [16].

Voice User Interfaces (VUIs): Voice user interfaces allow users to interact with IoMT applications using voice commands. This technology is particularly beneficial for patients with mobility challenges or those who prefer hands-free operation. VUIs can facilitate tasks such as setting reminders, querying health information, and controlling smart medical devices, enhancing accessibility and user experience [42].

Touchscreen Interfaces: Touchscreen interfaces are widely used in various medical devices and applications, providing an interactive way for users to engage with technology. These interfaces support gestures like tapping, swiping, and pinching, making it easier for users to navigate health applications, enter data, and access information quickly [42].

Augmented Reality (AR) and Virtual Reality (VR)

Augmented reality and virtual reality technologies are emerging in the healthcare sector, offering immersive experiences for training, education, and patient engagement. AR can overlay digital information onto the physical world, assisting healthcare professionals in procedures or patient education. VR can simulate clinical environments for training purposes, enhancing the learning experience for medical students and professionals [28].

Chatbots and Virtual Assistants: Chatbots and virtual assistants use artificial intelligence to provide users with instant responses to their health-related inquiries. These technologies can assist with appointment scheduling, medication reminders, and answering common health questions. By offering real-time support, chatbots enhance user experience and reduce the burden on healthcare staff [21].

Wearable Device Interfaces: Wearable devices, such as smartwatches and fitness trackers, feature user interfaces that allow users to monitor their health metrics in real time. These interfaces typically display information such as heart rate, activity levels, and sleep patterns. They often include notifications and alerts to keep users informed about their health status [36].

Feedback and Notification Systems: Feedback and notification systems alert users to important events, such as abnormal health readings or reminders for medications. These systems can use visual, auditory, or haptic feedback to ensure that users receive timely information. Effective notification systems enhance user engagement and promote adherence to health management plans [45].

2.6 Enabling Technologies in the Security Layer of IoMT

The security layer of the Internet of Medical Things (IoMT) is critical for protecting sensitive health data, ensuring patient privacy, and maintaining the integrity of medical devices and systems. This layer encompasses various technologies and practices designed to safeguard information and prevent unauthorized access. Here are the key enabling technologies in this layer:

Encryption Technologies: Encryption is a fundamental technology used to protect data at rest and in transit. It converts sensitive information into a coded format that can only be accessed by authorized users with the correct decryption key. Common encryption protocols include AES (Advanced Encryption Standard) for data storage and TLS (Transport Layer Security) for secure data transmission over networks. Access Control Mechanisms: Access control mechanisms regulate who can access specific data and resources within IoMT systems. These mechanisms include:

Role-Based Access Control (RBAC): Grants access based on user roles within an organization, ensuring that individuals only have access to the information necessary for their job functions.

Attribute-Based Access Control (ABAC): Uses policies that combine various attributes (e.g., user role, location, time) to determine access rights.

Multi-Factor Authentication (MFA): Requires users to provide multiple forms of verification (e.g., password and biometric data) before granting access, enhancing security.

Intrusion Detection and Prevention Systems (IDPS): Intrusion detection and prevention systems monitor network traffic for suspicious activities and potential threats. IDPS can identify unauthorized access attempts, malware, and other security breaches in real time. These systems can either alert administrators of potential threats (intrusion detection) or actively block malicious activities (intrusion prevention) [45].

Secure Communication Protocols: Secure communication protocols ensure that data transmitted between IoMT devices, applications, and servers is protected from interception and tampering. Protocols such as HTTPS (Hypertext Transfer Protocol Secure), MQTT (Message Queuing Telemetry Transport) with TLS, and secure Web Socket connections provide secure channels for data exchange in IoMT environments.

Figure 2: Enabling Technologies in IoMT

3.0 SECURITY CHALLENGES IN IOMT

The Internet of Medical Things (IoMT) integrates a vast network of interconnected medical devices, sensors, and systems to collect, transmit, and analyze health data, revolutionizing healthcare delivery. However, the complexity and sensitivity of this ecosystem introduce significant security challenges that threaten patient privacy, data integrity, and system reliability.

Data Privacy and Confidentiality: IoMT devices, including wearable fitness trackers, implantable sensors like pacemakers, and remote monitoring systems, continuously collect sensitive patient information such as vital signs, medical histories, and treatment details. This data, transmitted across wireless networks or stored in cloud platforms, is a prime target for malicious actors seeking to exploit it for financial gain or identity theft [33]. The reliance on communication protocols like Bluetooth, Wi-Fi, and 5G, which may not always be adequately secured, heightens the risk of unauthorized access or interception during transmission or storage. Ensuring confidentiality requires robust encryption and authentication mechanisms to prevent data exposure, as breaches could undermine patient trust and violate stringent regulations like HIPAA in the United States or GDPR in the European Union, which mandate rigorous data protection standards [45].

Data Integrity: The accuracy of health data is paramount in IoMT ecosystems, as medical decisions depend on the precision of information from biosensors, imaging systems, and smart textiles. Malicious tampering or manipulation, whether through cyberattacks or software vulnerabilities, could corrupt data, leading to incorrect diagnoses or inappropriate treatments. The interconnected nature of IoMT, where devices interface with cloud servers, electronic health records (EHRs), and clinical decision support systems, amplifies the potential for compromised data to propagate across the ecosystem, affecting healthcare providers and patients. Maintaining data integrity demands secure protocols and continuous monitoring to prevent unauthorized alterations that could jeopardize patient safety [37].

Device Security and Vulnerabilities: IoMT devices, such as wearables, environmental sensors, and hospital equipment, often have limited computational resources, making it challenging to implement advanced security features like real-time encryption or frequent firmware updates. Some devices may ship with default credentials or outdated software, exposing them to exploitation by hackers aiming to gain unauthorized control or disrupt functionality [20]. The widespread deployment of these devices across hospitals, homes, and public spaces further complicates security efforts, as physical access in unsecured environments increases the risk of tampering or theft, potentially allowing attackers to extract data or install malicious software, compromising the entire IoMT network [34].

Interoperability and Standardization Issues: The heterogeneity of IoMT systems, involving diverse devices, platforms, and protocols like MQTT, CoAP, or proprietary standards, creates significant security concerns. Inconsistent security practices across these systems result in vulnerabilities, as not all devices adhere to uniform security protocols. A single insecure device, such as a legacy medical imaging system, could serve as an entry point for attackers to infiltrate broader healthcare systems, including cloud platforms or EHR databases. Achieving interoperability while maintaining robust security requires standardized protocols and rigorous testing, a complex task given the rapid pace of IoMT adoption and the diversity of manufacturers involved [38].

Unauthorized Access and Authentication Weaknesses: Weak authentication mechanisms, such as simple passwords or lack of multi-factor authentication (MFA), increase the risk of unauthorized access to IoMT devices, applications, or data. Even advanced biometric identification systems, using fingerprints or facial recognition, can be vulnerable to spoofing or bypass techniques. User interfaces like mobile apps or web portals, critical for patient and provider interaction, are frequent targets for cyberattacks exploiting weak access controls. Without robust authentication, unauthorized users could access sensitive data or manipulate device settings, compromising patient care and system integrity across the IoMT ecosystem [37].

Network Security and Communication Risks: IoMT relies heavily on wireless communication technologies, including Bluetooth Low Energy, Zigbee, LoRaWAN, and cellular networks like 5G, to enable real-time data transfer between devices, gateways, and cloud servers [30]. These channels are susceptible to interception, eavesdropping, or man-in-the-middle attacks if not secured with protocols like TLS or HTTPS. In high-bandwidth applications like telemedicine or telesurgery, where low latency is critical, ensuring secure communication without compromising performance is particularly challenging. Insecure channels can expose sensitive data during transmission, especially in resource-constrained devices that may lack robust security implementations [6].

Scalability and Management of Security Updates: The scalability of IoMT deployments, with thousands of devices across healthcare settings, poses significant concerns for managing security updates and patches. Devices in remote or underserved areas, such as rural clinics, may not receive timely firmware updates, leaving them exposed to known vulnerabilities or emerging threats. The projected growth of the IoMT market, from USD 48.7 billion in 2022 to USD 370.9 billion by 2032, underscores the urgency of implementing scalable security solutions. Without centralized management systems, ensuring consistent security across diverse, distributed devices becomes increasingly difficult, heightening the risk of exploitation [35].

Regulatory Compliance: IoMT systems must adhere to stringent regulatory frameworks like HIPAA and GDPR, which mandate robust data protection, encryption, and patient consent practices. Navigating these requirements across a complex ecosystem of devices, cloud platforms, and third-party applications is resource-intensive, particularly given variations in regional regulations. Ensuring compliance involves implementing secure data handling, conducting regular audits, and maintaining transparency, but inconsistencies in adherence across diverse systems can weaken overall security, exposing organizations to legal and reputational risks while complicating efforts to protect patient data [31].

Insider Threats: Authorized users, such as healthcare staff or third-party vendors, can inadvertently or maliciously compromise IoMT systems through negligence, such as using weak passwords or sharing credentials, or intentional misuse, such as unauthorized data access. In healthcare settings, where staff interact with sensitive systems like EHRs or clinical dashboards, these threats are particularly concerning. Robust access controls, user training, and monitoring are essential to mitigate risks, but the human element remains a significant vulnerability in securing IoMT ecosystems, as insider actions can bypass external security measures like encryption or intrusion detection [39].

Data Overload and Analytics Security: IoMT generates massive volumes of data processed through cloud computing, edge computing, and AI-driven analytics platforms, such as those using Apache Hadoop or machine learning algorithms. Securing these data processing pipelines is critical, as vulnerabilities in storage or processing algorithms can expose aggregated patient data. AI systems are particularly susceptible to adversarial attacks that manipulate inputs to produce inaccurate outputs, potentially affecting diagnostic accuracy or treatment recommendations. Ensuring the security of these complex analytics systems is essential to maintain trust in IoMT-driven healthcare solutions [34].

Physical Security of Devices: IoMT devices deployed in non-clinical settings, such as patients' homes or public spaces, are vulnerable to physical tampering or theft. Wearables, environmental sensors, or remote monitoring devices, if accessed by malicious actors, could be used to extract data or disrupt the IoMT network. Securing these devices in distributed environments requires tamper-resistant hardware and remote disabling capabilities, but the widespread deployment of IoMT devices makes physical security a persistent concern, particularly for devices with limited built-in protections [37].

Emerging Threats from Advanced Technologies: The integration of advanced technologies like blockchain, augmented reality (AR), and Bio-Nano Things into IoMT systems introduces new security complexities. Blockchain, used for secure data management, requires meticulous key management to prevent unauthorized access. AR and VR applications, employed for training or patient engagement, may expose new attack vectors if not properly secured. Bio-Nano Things, operating at the molecular level, face unique challenges due to their limited computational capabilities, necessitating innovative security approaches to safeguard their functionality. As these technologies evolve, they bring novel risks that require proactive measures to ensure the security of the IoMT ecosystem [30].

Figure 3: Security Challenges and their Mitigation

4 DISCUSSION AND CONCLUSION

4.1 Discussion

The Internet of Medical Things (IoMT) leverages interconnected devices, such as biosensors, wearables, and cloud-based analytics, to revolutionize healthcare, but its complexity introduces significant security challenges that threaten patient data and system reliability. Sensitive health information collected across device, connectivity, and data processing layers is vulnerable to unauthorized access, tampering, or interception, particularly through insecure protocols like Bluetooth or Wi-Fi, while resource-constrained devices struggle to support robust encryption or updates, and heterogeneous systems lack uniform security standards, risking network-wide vulnerabilities. Authentication weaknesses, insider threats, and emerging risks from technologies like AI and Bio-Nano Things further complicate the landscape, as do scalability issues in managing thousands of devices and compliance with regulations like HIPAA and GDPR. Mitigation strategies, including AES-256 encryption, multi-factor authentication, HL7/FHIR standards, blockchain, and intrusion detection systems, offer effective defences, but their implementation requires overcoming logistical barriers, ensuring interoperability, and fostering collaboration among manufacturers, providers, and policymakers to maintain trust and safety in IoMT-driven healthcare.

4.2 Conclusion

The IoMT ecosystem, while transformative for healthcare through its real-time monitoring and advanced analytics, faces critical security challenges, including data breaches, device vulnerabilities, and regulatory complexities, necessitating robust mitigations like encryption, standardized protocols, and user training to ensure patient safety and data integrity. As the IoMT market grows, stakeholders must prioritize unified security standards, scalable update systems, and innovative solutions for emerging technologies like AI and blockchain, while fostering collaboration and awareness to address evolving cyber threats, ensuring IoMT fulfils its potential as a secure and reliable cornerstone of modern healthcare.

5 RECOMMENDATION AND FURTHER RESEARCH

5.1 Recommendations

To strengthen the security of the Internet of Medical Things (IoMT) ecosystem, stakeholders—including device manufacturers, healthcare providers, and policymakers—should adopt a comprehensive, multi-layered approach that integrates robust technical, procedural, and regulatory measures across all IoMT layers, from devices to user interfaces. Implementing AES-256 encryption and Transport Layer Security (TLS) for data protection, alongside multi-factor authentication (MFA) and role-based access control (RBAC), can safeguard sensitive health data collected by biosensors, wearables, and remote monitoring systems against unauthorized access and tampering. Manufacturers must prioritize designing devices with sufficient computational resources to support regular firmware updates and tamper-resistant features, particularly for those deployed in unsecured environments like patients' homes. Adopting standardized protocols like HL7 and FHIR will enhance interoperability and reduce vulnerabilities caused by inconsistent security practices across diverse devices and platforms. Healthcare organizations should invest in centralized update systems and intrusion detection solutions to manage scalability challenges, while comprehensive training programs for staff and patients can mitigate insider threats and promote security awareness. Policymakers should foster collaboration through regulatory frameworks that incentivize uniform security standards and compliance with HIPAA and GDPR, ensuring a cohesive approach to protect patient trust and safety in IoMT-driven healthcare.

5.2 Further research

Future research is essential to address the evolving security challenges of the IoMT ecosystem, particularly as emerging technologies like blockchain, augmented reality (AR), and Bio-Nano Things introduce new complexities. Investigating lightweight encryption algorithms and energy-efficient security protocols tailored for resource-constrained devices, such as ingestible sensors and Bio-Nano Things, will be critical to balancing security with performance. Research into advanced AI model validation techniques is needed to counter adversarial attacks that could compromise data analytics and diagnostic accuracy in cloud and edge computing environments. Exploring scalable blockchain implementations with secure key management can enhance data integrity and patient consent mechanisms, but studies must address their practicality in large-scale IoMT deployments. Additionally, developing adaptive intrusion detection systems that leverage machine learning to detect and respond to real-time threats across heterogeneous networks, including 5G and LoRaWAN, warrants further exploration. Research should also focus on user-centric security solutions, such as intuitive authentication methods for non-technical users interacting with mobile apps or voice interfaces, and the effectiveness of regulatory frameworks in promoting global interoperability while maintaining robust security, ensuring IoMT systems remain resilient against future cyber threats.

FUNDING

The research conducted for this study did not receive any financial support or funding from external sources

COMPETING INTERE ST

The authors have explicitly stated that they have no competing interests related to this research.

6. REFERENCE

1. R. Yadav, P. Pradeepa, S. Srinivasan, C. S. Rajora, and R. Rajalakshmi, "A novel healthcare framework for ambient assisted living using the internet of medical things (IOMT) and deep neural network," Meas. Sens., vol. 33, p. 101111, June 2024, doi: 10.1016/j.measen.2024.101111.
2. S. Subha, T. M. Inbamalar, K. C. R, L. R. Suresh, S. Boopathi, and K. Alaskar, "A Remote Health Care Monitoring system using internet of medical things (IoMT)," in 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM), Uttar Pradesh, India: IEEE, Feb. 2023, pp. 1–6. doi: 10.1109/ICIPTM57143.2023.10118103.
3. Z. Ashfaq et al., "A review of enabling technologies for Internet of Medical Things (IoMT) Ecosystem," Ain Shams Eng. J., vol. 13, no. 4, p. 101660, June 2022, doi: 10.1016/j.asej.2021.101660.
4. O. AlShorman, B. AlShorman, M. Al-khassaweneh, and F. Alkahtani, "A review of internet of medical things (IoMT) - based remote health monitoring through wearable sensors: a case study for diabetic patients," Indones. J. Electr. Eng. Comput. Sci., vol. 20, no. 1, p. 414, Oct. 2020, doi: 10.11591/ijeecs.v20.i1.pp414-422.
5. M. Papaioannou et al., "A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT)," Trans. Emerg. Telecommun. Technol., vol. 33, no. 6, p. e4049, June 2022, doi: 10.1002/ett.4049.
6. T. Ahmed Alhaj et al., "A Survey: To Govern, Protect, and Detect Security Principles on Internet of

Medical Things (IoMT),” IEEE Access, vol. 10, pp. 124777–124791, 2022, doi: 10.1109/ACCESS.2022.3225038.
7. R. Rawat, “A SYSTEMATIC REVIEW OF BLOCKCHAIN TECHNOLOGY USE IN E-SUPPLY CHAIN IN INTERNET OF MEDICAL THINGS (IOMT),” Int. J. Comput. Inf. Manuf. IJCIM, vol. 2, no. 2, Nov. 2022, doi: 10.54489/ijcim.v2i2.119.
8. I. V. Pustokhina, D. A. Pustokhin, D. Gupta, A. Khanna, K. Shankar, and G. N. Nguyen, “An Effective Training Scheme for Deep Neural Network in Edge Computing Enabled Internet of Medical Things (IoMT) Systems,” IEEE Access, vol. 8, pp. 107112–107123, 2020, doi: 10.1109/ACCESS.2020.3000322.
9. A. C. B. Monteiro, R. P. França, R. Arthur, and Y. Iano, “An overview of the Internet of medical things (IoMT): Applications, benefits, and challenges,” in Security and Privacy Issues in Internet of Medical Things, Elsevier, 2023, pp. 83–98. doi: 10.1016/B978-0-323-89872-0.00009-5.
10. B. Kim, S. Kim, M. Lee, H. Chang, E. Park, and T. Han, “Application of an Internet of Medical Things (IoMT) to Communications in a Hospital Environment,” Appl. Sci., vol. 12, no. 23, p. 12042, Nov. 2022, doi: 10.3390/app122312042.
11. P. Manickam et al., “Artificial Intelligence (AI) and Internet of Medical Things (IoMT) Assisted Biomedical Systems for Intelligent Healthcare,” Biosensors, vol. 12, no. 8, p. 562, July 2022, doi: 10.3390/bios12080562.
12. C. Anitha, K. C. R, C. V. Vivekanand, S. D. Lalitha, S. Boopathi, and Revathi. R, “Artificial Intelligence driven security model for Internet of Medical Things (IoMT),” in 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM), Uttar Pradesh, India: IEEE, Feb. 2023, pp. 1–7. doi: 10.1109/ICIPTM57143.2023.10117713.
13. V. S. Parvathy, S. Pothiraj, and J. Sampson, “Automated Internet of Medical Things (IoMT) Based Healthcare Monitoring System,” in Cognitive Internet of Medical Things for Smart Healthcare, vol. 311, A. E. Hassanien, A. Khamparia, D. Gupta, K. Shankar, and A. Slowik, Eds., in Studies in Systems, Decision and Control, vol. 311. , Cham: Springer International Publishing, 2021, pp. 117–128. doi: 10.1007/978-3-030-55833-8_7.
14. S. Alam et al., “Blockchain-Based Solutions Supporting Reliable Healthcare for Fog Computing and Internet of Medical Things (IoMT) Integration,” Sustainability, vol. 14, no. 22, p. 15312, Nov. 2022, doi: 10.3390/su142215312.
15. T. Yang, M. Gentile, C.-F. Shen, and C.-M. Cheng, “Combining Point-of-Care Diagnostics and Internet of Medical Things (IoMT) to Combat the COVID-19 Pandemic,” Diagnostics, vol. 10, no. 4, p. 224, Apr. 2020, doi: 10.3390/diagnostics10040224.
16. S. K. Udgata and N. K. Suryadevara, “COVID-19, Sensors, and Internet of Medical Things (IoMT),” in Internet of Things and Sensor Network for COVID-19, in SpringerBriefs in Applied Sciences and Technology. , Singapore: Springer Singapore, 2021, pp. 39–53. doi: 10.1007/978-981-15-7654-6_3.
17. I. Irkham, A. U. Ibrahim, C. W. Nwekwo, F. Al-Turjman, and Y. W. Hartati, “Current Technologies for Detection of COVID-19: Biosensors, Artificial Intelligence and Internet of Medical Things (IoMT): Review,” Sensors, vol. 23, no. 1, p. 426, Dec. 2022, doi: 10.3390/s23010426.
18. A. Khang, G. Rana, R. K. Tailor, and V. Abdullayev, Eds., Data-centric AI solutions and emerging technologies in the healthcare ecosystem, First edition. Boca Raton: CRC Press, 2024.
19. A. Kumar, D. Chaturvedi, and S. I. Rosaline, “Design of Antenna-Multiplexer for Seamless On-Body Internet of Medical Things (IoMT) Connectivity,” IEEE Trans. Circuits Syst. II Express Briefs, vol. 69, no. 8, pp. 3395–3399, Aug. 2022, doi: 10.1109/TCSII.2022.3170513.
20. M. Alalhareth and S.-C. Hong, “Enhancing the Internet of Medical Things (IoMT) Security with Meta-Learning: A Performance-Driven Approach for Ensemble Intrusion Detection Systems,” Sensors, vol. 24, no. 11, p. 3519, May 2024, doi: 10.3390/s24113519.
21. Md. N. Hossen, V. Panneerselvam, D. Koundal, K. Ahmed, F. M. Bui, and S. M. Ibrahim, “Federated Machine Learning for Detection of Skin Diseases and Enhancement of Internet of Medical Things (IoMT) Security,” IEEE J. Biomed. Health Inform., vol. 27, no. 2, pp. 835–841, Feb. 2023, doi: 10.1109/JBHI.2022.3149288.
22. C. Dilibal, B. L. Davis, and C. Chakraborty, “Generative Design Methodology for Internet of Medical Things (IoMT)-based Wearable Biomedical Devices,” in 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey: IEEE, June 2021, pp. 1–4. doi: 10.1109/HORA52670.2021.9461370.
23. K. K. Baseer et al., “Healthcare diagnostics with an adaptive deep learning model integrated with the Internet of medical Things (IoMT) for predicting heart disease,” Biomed. Signal Process. Control, vol. 92, p. 105988, June 2024, doi: 10.1016/j.bspc.2024.105988.

24. S. F. Ahmed, Md. S. B. Alam, S. Afrin, S. J. Rafa, N. Rafa, and A. H. Gandomi, "Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions," Inf. Fusion, vol. 102, p. 102060, Feb. 2024, doi: 10.1016/j.inffus.2023.102060.
25. R. Pratap Singh, M. Javaid, A. Haleem, R. Vaishya, and S. Ali, "Internet of Medical Things (IoMT) for orthopaedic in COVID-19 pandemic: Roles, challenges, and applications," J. Clin. Orthop. Trauma, vol. 11, no. 4, pp. 713–717, July 2020, doi: 10.1016/j.jcot.2020.05.011.
26. R. A. Osman, "Internet of Medical Things (IoMT) optimization for healthcare: A deep learning-based interference avoidance model," Comput. Netw., vol. 248, p. 110491, June 2024, doi: 10.1016/j.comnet.2024.110491.
27. A. Saxena and S. Mittal, "Internet of Medical Things (IoMT) Security and Privacy: A Survey of Recent Advances and Enabling Technologies," in Proceedings of the 2022 Fourteenth International Conference on Contemporary Computing, Noida India: ACM, Aug. 2022, pp. 550–559. doi: 10.1145/3549206.3549301.
28. 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," in Intelligent Healthcare, C. Chakraborty and M. R. Khosravi, Eds., Singapore: Springer Nature Singapore, 2022, pp. 299–319. doi: 10.1007/978-981-16-8150-9_14.
29. S. Razdan and S. Sharma, "Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies," IETE Tech. Rev., vol. 39, no. 4, pp. 775–788, July 2022, doi: 10.1080/02564602.2021.1927863.
30. A. A. Karam, "INVESTIGATING THE IMPORTANCE OF ETHICS AND SECURITY ON INTERNET OF MEDICAL THINGS (IoMT)," Int. J. Comput. Inf. Manuf. IJCIM, vol. 2, no. 2, Nov. 2022, doi: 10.54489/ijcim.v2i2.114.
31. G. S. Aljumaie, G. H. Alzeer, R. K. Alghamdi, H. Alsuwat, and E. Alsuwat, "Modern Study on Internet of Medical Things (IOMT) Security," Int. J. Comput. Sci. Netw. Secur., vol. 21, no. 8, pp. 254–266, Aug. 2021, doi: 10.22937/IJCSNS.2021.21.8.34.
32. D. M. Mathkor et al., "Multirole of the internet of medical things (IoMT) in biomedical systems for managing smart healthcare systems: An overview of current and future innovative trends," J. Infect. Public Health, vol. 17, no. 4, pp. 559–572, Apr. 2024, doi: 10.1016/j.jiph.2024.01.013.
33. 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. Craniofacial Res., vol. 12, no. 2, pp. 302–318, Mar. 2022, doi: 10.1016/j.jobcr.2021.11.010.
34. A. S. Rajawat, S. B. Goyal, P. Bedi, T. Jan, M. Whaiduzzaman, and M. Prasad, "Quantum Machine Learning for Security Assessment in the Internet of Medical Things (IoMT)," Future Internet, vol. 15, no. 8, p. 271, Aug. 2023, doi: 10.3390/fi15080271.
35. A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security," IEEE Internet Things J., vol. 8, no. 11, pp. 8707–8718, June 2021, doi: 10.1109/JIOT.2020.3045653.
36. . Lin, X. Li, K. Cai, M. Prakash, and D. Paulraj, "Secure Internet of medical Things (IoMT) based on ECMQV-MAC authentication protocol and EKMC-SCP blockchain networking," Inf. Sci., vol. 654, p. 119783, Jan. 2024, doi: 10.1016/j.ins.2023.119783.
37. R. Hireche, H. Mansouri, and A.-S. K. Pathan, "Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis," J. Cybersecurity Priv., vol. 2, no. 3, pp. 640–661, Aug. 2022, doi: 10.3390/jcp2030033.
38. A. A. El-Saleh, A. M. Sheikh, M. A. M. Albreem, and M. S. Honnurvali, "The Internet of Medical Things (IoMT): opportunities and challenges," Wirel. Netw., vol. 31, no. 1, pp. 327–344, Jan. 2025, doi: 10.1007/s11276-024-03764-8.
39. B. Bhushan, A. Kumar, A. K. Agarwal, A. Kumar, P. Bhattacharya, and A. Kumar, "Towards a Secure and Sustainable Internet of Medical Things (IoMT): Requirements, Design Challenges, Security Techniques, and Future Trends," Sustainability, vol. 15, no. 7, p. 6177, Apr. 2023, doi: 10.3390/su15076177.
40. K. K. Karmakar, V. Varadharajan, U. Tupakula, S. Nepal, and C. Thapa, "Towards a Security Enhanced Virtualised Network Infrastructure for Internet of Medical Things (IoMT)," in 2020 6th IEEE Conference on Network Softwarization (NetSoft), Ghent, Belgium: IEEE, June 2020, pp. 257–261. doi: 10.1109/NetSoft48620.2020.9165387.
41. R. Kumar and R. Tripathi, "Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology," J. Supercomput., vol. 77, no. 8, pp. 7916–7955, Aug. 2021, doi: 10.1007/s11227-020-03570-x.
42. A. A. Aljabr and K. Kumar, "Design and implementation of Internet of Medical Things

(IoMT) using artificial intelligent for mobile-healthcare," Meas. Sens., vol. 24, p. 100499, Dec. 2022, doi: 10.1016/j.measen.2022.100499.

43. S. Jain et al., "Internet of medical things (IoMT)-integrated biosensors for point-of-care testing of infectious diseases," Biosens. Bioelectron., vol. 179, p. 113074, May 2021, doi: 10.1016/j.bios.2021.113074.
44. S. Vishnu, S. R. J. Ramson, and R. Jegan, "Internet of Medical Things (IoMT) - An overview," in 2020 5th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India: IEEE, Mar. 2020, pp. 101–104. doi: 10.1109/ICDCS48716.2020.243558.
45. J. Srivastava, S. Routray, S. Ahmad, and M. M. Waris, "Internet of Medical Things (IoMT)-Based Smart Healthcare System: Trends and Progress," Comput. Intell. Neurosci., vol. 2022, pp. 1–17, July 2022, doi: 10.1155/2022/7218113.