A Comprehensive Literature Survey on the Internet of Medical Things (IoMT): Challenges, Research Gaps, and Future Directions

Mallikarjuna Reddy B[1*] and R. Rajasekhar[2]
{ berammkr@gmail.com[1*], drasharaj2002.cse@jntua.ac.in[2]}

Research Scholar, Department of CSE, JNTUA College of Engineering, Ananthapuramu, Andhra Pradesh, India[1]
Professor, Department of CSE, JNTUA College of Engineering, Ananthapuramu, Andhra Pradesh, India[2]

Abstract. The IOMT and big data are newer technologies that can provide extensive support for healthcare systems, helping them overcome shortcomings. Health is a common objective pursued by all human beings and people's health is the primary responsibility in medical systems. As medical techniques and philosophy advance, systems require technologies to develop new ways to prevent and treat diseases and improve resilience to public health crises. Technology advancement drives the growth of Internet of Things (IoT) applications in many fields, including healthcare. IoT in healthcare is called the Internet of Medical Things (IOMT), an emerging subset of IoT referring to medical devices and applications with internet connectivity. IOMT has revolutionized healthcare services by providing significant benefits in patient well-being and costs. IOMT devices transmit health or technical data to cloud or internal servers to monitor patient health parameters and help prevent, diagnosing or treat diseases. IOMT expedites remote health biomedical systems and enhances precision, reliability, consistency and productivity of electronic devices used for healthcare purposes. The integration of AI & ML and Big Data Analytics holds a substantial promise for transforming healthcare systems. AI & ML capability in complex data analysis combined with advanced big data analytics models achieves efficient processing of large amounts of data in a very short time. IoMT faces major challenges, including security vulnerabilities, lack of interoperability, and scalability constraints in handling massive real-time healthcare data. Energy inefficiency in devices, AI transparency issues, and regulatory hurdles (HIPAA, GDPR) further limit adoption. Machine learning (ML) and deep learning (DL) models, though promising, often function as "black boxes," reducing clinical trust. Integration with legacy healthcare systems remains difficult due to outdated IT infrastructure and incompatible vendor platforms. Future research should focus on blockchain-based security, universal interoperability standards (HL7, FHIR), and cloud-edge hybrid architectures for scalable data processing. ML and DL-driven predictive analytics can enhance diagnostics, but explainable AI (XAI) is crucial for clinician trust. Energy-efficient IoMT hardware and privacy-preserving AI will ensure long-term usability and compliance. Integrating IoMT with Healthcare 5.0 technologies (5G, AR/VR, and robotics) will enable real-time, personalized, and globally connected healthcare.

Keywords: IoMT, IoT, Big Data Analytics, Healthcare, Research Gaps, Challenges, Future Directions.

1 Introduction

As a tool of smart healthcare, sensors are very important as smart devices that measure heart rate, blood pressure, sleep patterns, body temperature, brain activity and other data related to

ICITSM-Part II 2025, April 28-29, Tiruchengode, India
Copyright © 2025 EAI
DOI 10.4108/eai.28-4-2025.2357980

health. The Internet of Things (IoT) is open out from connecting individual devices to the internet and creating smart software systems and then automates the process and same has been transformed to the industries [1][2]. The Internet of Medical Things (IOMT) is a subset of IOT and is specially designed for healthcare systems and enable telehealth and other medical devices. The evolution from IOT to IOMT represents a specialized branch and it focuses on the integration of smart devices, sensors, and a medical technology to revolutionize healthcare sector. Recognizing the unique requirements and opportunities within the healthcare sector drives the evolution of IOT to IOMT. IOMT provide the solutions to the problems faced by outdated medical systems like lack of healthcare resources, doctors. Research data collected through IOMT used by the researchers to diagnose and predict diseases. IOMT mainly focuses on exploiting IOT technologies, methods and principles to enhance healthcare industry, improve patient outcomes, and provide patient centric care while addressing the healthcare industry's specific challenges and regulatory considerations [3].

The transformation from the IOT to the IOMT is not just semantic shift and it represents a significant adaptation of technology to meet the specific needs of healthcare. IOMT will provides huge data and giving to medical clinicians for more accurate insights into the health conditions of patients. The server is the back bone of an IOMT system.

IOT is very deep into medical system and then rise to new model of the IOMT. IOMT is also known as Internet of things in healthcare. IOMT is the hot technology filed in the healthcare industry. IOMT devices create a connected healthcare network by facilitating the continuous flow of patient data. The range of interconnected medical devices continuously collects health data from patients via sensors and transferring to healthcare providers, such as doctors and hospitals. IOMT devices collect the crucial signs of patients to store on the cloud by aggregating them into medical data files. Healthcare workers can access them the same. Regular monitoring of patients through wearable devices and sensors gained attention. IOMT brings improvements in live of patients in clinician's work and health systems. It is very beneficial to examine as a practical scenario. Recent days IOMT is applying many areas like smart hospital, remote health monitoring, disease diagnosis, infectious disease monitoring [4].

AI enhances IOT devices by providing intelligence for data analysis and decision making. AI algorithms process data from sensors, identifying patterns, anomalies and trends in real time. It enables predictive analytics and also identifying future events based on historical data. The role of big data, AI-ML and parallel computing is creating digitals twins for various industrial applications in various levels. In the modern world the use of IoT, big data, parallel computing, AI-ML technologies had brought new power [5].

The increasing demand for efficient and personalized healthcare solutions in IoMT (Internet of Medical Things) stems from rapid advancements in AI, IoT, and 5G technologies, as well as a global focus on improving healthcare outcomes. IoMT enables real-time monitoring, data collection, and analysis, facilitating remote diagnostics, predictive analytics, and comprehensive health management [6].

1.1 Key drivers of this demand include:

- Personalization: Individualizing treatment for each patient through genomic, environmental and lifestyle factors, for better results in a patient with multiple or chronic conditions.

- Reliability and resiliency: having the ability and capacity to maintain health care services in a reliable and consistent manner, even in the presence of adverse events, so that clinical monitoring and treatment are continuous and accurate.

- Interoperability: Ensuring a seamless connection between different medical devices and systems for meaningful data sharing and insights to support more informed decision making.

There is a growing need to develop effective personalized health care in IoMT, overcoming the constraints/limitations of traditional systems and embracing the developments in healthcare 5.0. The Internet of Medical things (IoMT) is transforming healthcare delivery because of its potential to converge innovative technologies and deliver tailored and timely care. Its transformative possibilities are:

IoMT supports constant collection of information from connected devices, which helps to monitor patient health in near real-time. It helps to detect early onset of serious conditions such as heart and diabetes, preventing hospitalization and improving health. Applications vary from point-of-care biosensors for the detection of infectious diseases, wearable devices for monitoring chronic diseases, AI-based diagnostic tools, and so on [7].

With AI and machine learning, IoMT customizes physicians' interventions to patient needs. For example, IoMT systems empowered with AI achieve high precision in the prediction of diseases and the customization of interventions. These systems consider genetic, behavioural, and environmental characteristics to provide a determinant-based optimization of healthcare.

The Internet of Medical Things (IoMT) is transforming health care by driving patient engagement, operational efficiencies, and the management of at-risk populations with by enabling real-time monitoring and customized care. But its scalability, security and integration are very difficult. IoMT produces large amounts of data, for which scalable technologies such as the cloud, the edge, and fog are necessary and, at the same time, there is a need to deal with interoperability as a result of different formats and communications protocols. Barriers such as limited network bandwidth, power consumption, and blockchain scalability have also made it difficult for the implementation on a large scale. Privacy and patient safety are at risk from malicious access, ransomware and weak encryption. Conformance with the regulatory frameworks such as HIPAA and GDPR also increases complexity and the integration of IoMT solutions with existing healthcare systems is challenging, due to technology heterogeneity and deployment costs. The future research needs to target on the improvements of blockchain scalability, the construction of uniform communication protocols, and the utilization of AI-based security mechanisms for the efficient, security and authorization of the IoMT in the world-wide medical systems.

The Internet of Medical Things (IoMT) is changing healthcare through real-time monitoring, data-based decision-making, and improved patient outcomes. This work also aims to take a systematic review over the IoMT field and investigates the value of monitoring, integrating data from the healthcare, as well as the process efficiency for healthcare organization. However, despite its promise, many significant issues remain, including security concerns, standardization issues, data management, and ethical issues. The primary research challenges include lack of strong security paradigms, huge interoperability based on heterogenous IoMT devices, and requirement for scalable solutions with energy efficiency. Furthermore, explainability, trust, and cognitive health applications are among the challenges for AI-based

IoMT systems. In addressing these deficiencies, actionable research directions are highlighted including development of standardised security frameworks, AI and blockchain fusion, real-time analytics, and ethical governance frameworks. Such knowledge bridges can leverage IoMT's scalability, security and relevance to global patient-centered care and lead to IoMTs' constitute adoption and sustainable impact [8].

1.2 Key Contributions of the Paper

- Review of the IoMT Space – Offers a detailed study of the applications of IoMT in healthcare, with an emphasis on real-time monitoring, data driven decisions and patient centric care.
- Challenges and Research Gaps – Identifies some of the most critical issues critical issues related to lack of security, lack of interoperability, data management issues, and ethical issues as challenges for adopting IoMT.
- Proposed Actionable Research Directions – recommends various solutions that include, but are not limited to, standard security frameworks, AI-enabled real-time analytics, sustainable IoMT device design, and secure data sharing using blockchain.
- Future-Proofing IoMT for Scalable Healthcare Solutions – Leverages IoT in healthcare with the latest technology trends such as AI, 5G, and Healthcare 4.0/5.0 in optimizing predictive analytics, telemedicine, and customizable healthcare.

2 Background Study

Internet of Medical Things (IoMT) links medical devices and health systems through internet, supports remote monitoring and collects real-time data. It improves patient care and saves money, and its telemedicine-friendly. But security and compatibility issues still stump the average user.

2.1 Overview of IoMT

Extending IoT to IoMT: Going beyond explicit patient consent the transformation of IoT into Internet of Medical Things (IoMT) marks a quantum leap in health technology. If IoT created the base infrastructure of connected devices, then IoMT provided the differentiation of that infrastructure to meet healthcare needs. With the development of AI, 5G and data analysis, IoMT is ready to transform patient care, enhance healthcare outcomes and streamline the operations within healthcare. But the use of AI and big data also have several data privacy, security, and regulatory compliance issues that need to be resolved to unlock its full value.

Internet of medical things is an application that collects and sends medical data from the device on a network. additional information shared with medical practitioners for a more precise diagnosis of the patient's health situation. Examples of such include that an IOMT enabled BP meter containing readings for the past several days can deliver a quicker and a more accurate diagnosis than readings corresponding from single doctor visit [9].

Architecture IOMT with four layers as illustrated in Fig 1. The architecture of Internet of Medical Things (IoMT) consists of four layers based on effective hospital monitoring. The Sensor Layer consists of wearable and environment sensors to capture real-time physiological information. The Gateway Layer makes the data processing smooth over Wi-Fi, ZigBee and

Bluetooth protocols. Data is processed and stored in a cloud-based server and database by the Cloud Service Layer. Lastly, the Application Layer offers a user interface for those at the end-points (clinicians and families) to ensure remote monitoring and decision support. It improves interoperability, scalable solutions, and real-time health management by using a structured methodology.

2.2 Technological Landscape of IoMT

The technological landscape of IoMT includes smart medical devices, wearable sensors, cloud computing, AI-driven analytics, and 5G connectivity. These technologies enable real-time monitoring, remote diagnostics, and personalized healthcare. Advancements in cyber security, blockchain, and interoperability solutions are enhancing data security and seamless integration across healthcare systems.

2.2.1 IoMT Devices and Architecture

The Internet of Medical Things (IoMT) is a connected infrastructure of medical devices, software applications, and health systems and services that collect and monitor patient health data to improve patient service delivery and efficiency. Wearable, implantable and connected health IoMT Aspects Devices in the IoMT can be divided into wearables, implantable and connected health systems. Wearables, such as Smartwatches and continuous glucose monitors, provide health tracking in real time for proactive health management. Pacemakers and Neurostimulators, being implanted devices, allow long term monitoring and treatment of chronical diseases. Integrated health systems combine IoMT data with healthcare providers, enabling remote patient monitoring, telemedicine and intelligent hospital equipment. These are the technologies designed to empower patients and clinicians and streamline healthcare.

The IoMT architecture is organized around four main layers: the sensor layer, which acquires real-time physiological and environmental data; the gateway (edge/fog computing) layer, which pre-processes data, reduces latency, and increases security; the cloud layer, for largescale data storage, analytics, and remote access; and the application layer, to support healthcare decision making with telemedicine, personal-health apps, and real-time alarm management. The secure and efficient communication in IoMT is based on TLS, mutual authentication, and encryption techniques, and wireless technologies like BLE, Wi-Fi, 5 G, Zigbee, and NFC. Burgeoning blockchain facilities are also improving data integrity and security. These improvements enhance the efficiency of healthcare and facilitate real-time monitoring, and at the same time get better patient outcomes and patient data privacy and interoperability [10][36].

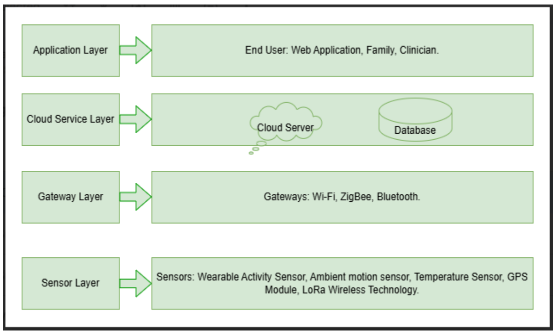
Application Layer
End User: Web Application, Family, Clinician.
Cloud Service Layer
Cloud Server
Database
Gateway Layer
Gateways: Wi-Fi, ZigBee, Bluetooth.
Sensor Layer
Sensors: Wearable Activity Sensor, Ambient motion sensor, Temperature Sensor, GPS Module, LoRa Wireless Technology.

Fig. 1. IoMT Architecture for Healthcare Systems.

2.2.2 Role of Big Data and AI

Big data analytics and AI are revolutionizing healthcare through the use of copious data collected from IoMT devices to enhance patient outcomes, predict diseases, and tailor treatments. IoMT covers medical devices (wearables, smart implants) which support real-time data that is stored in the cloud and that can be analysed with cloud computing and machine learning. AI prediction diagnostics AI and drug/medical treatments plan Personalized AI-driven predictive diagnostics AI-driven predictive diagnostics facilitate early detection of disease by employing sophisticated models like the thing666(IV) ADV model and SVM, while treatment applications tailor patient care through reinforcement learning and PGx 11. AI also facilitates real-time anomaly detection and remote monitoring, lessening hospital visits and enhancing healthcare efficiency. Nevertheless, there are barriers waiting for being solved, including data safety and privacy protection, interoperation, and model efficacy, before the benefits of the AI-and-big-data-based healthcare can be effectively harnessed [13].

2.2.3 Cloud and Edge Computing

Cloud and edge computing are instrumental in improving the scalability, efficiency, and real-time processing performance of the Internet of Medical Things (IoMT) [14]. Cloud computing offers a means to centralize storage and analysis of medical data as well remote monitoring of the patient, and supports interoperability and scalability. But given vulnerabilities and delay and reliance on third party vendors, new solutions are needed. Edge computing resolves these problems by enabling data to be processed at source, which reduces latency, saves bandwidth and allows for real-time decision-making in life-critical applications such as cardiac monitoring and remote surgery. Furthermore, computation offloading at the edge improves the energy consumption, and prolongs the battery lifetime of IoMT devices. Although the data management is achieved on a large scale by cloud computing, it will guarantee security, privacy, and response time via both blockchain and edge computing. Cloud, edge and AI based analytics, especially when combined with 5G could address critical healthcare delivery challenges and provide great innovations, but issues associated with inter-node communication, scalability and cost are hindering further adoption 1517.

2.3 Use Cases in Healthcare

The internet of medical things (IoMT) is the connected system of medical devices and applications that collect, analyse, and transmit health data over the internet. Top use cases include: Remote Patient monitoring, Smart wearables and implantable devices, P4 Medicine (Predictive, Preventive, Personalized, and Participatory), Disease diagnosis and management through IoMT, Telemedicine & virtual care, Emergency Response Systems, Smart Ambulances, Smart Surgical Instruments and Connected Contact Lenses.

Fig 2 illustrates that, the IoMT applications in eHealth are mostly concentrated in Remote Patient Monitoring (25%), followed by Wearable Health Devices (20%) [74] and, Smart Hospitals (15%); where smart hospitals mean optimizing the patient tracking and operation of a healthcare facility. Telemedicine & Virtual Care (10%) and Medication Management (10%) improve teleconsultations and therapy compliance. It also provides real-time health monitoring and long-term care services (Emergency Response Systems 8% and Chronic Disease Management 7%). AI diagnostics and smart surgeries (5%) are other applications that enhance operational efficiency in healthcare. This spread highlights the scale of IoMT in improving patient outcomes, streamlining hospital services, and improving medical results.

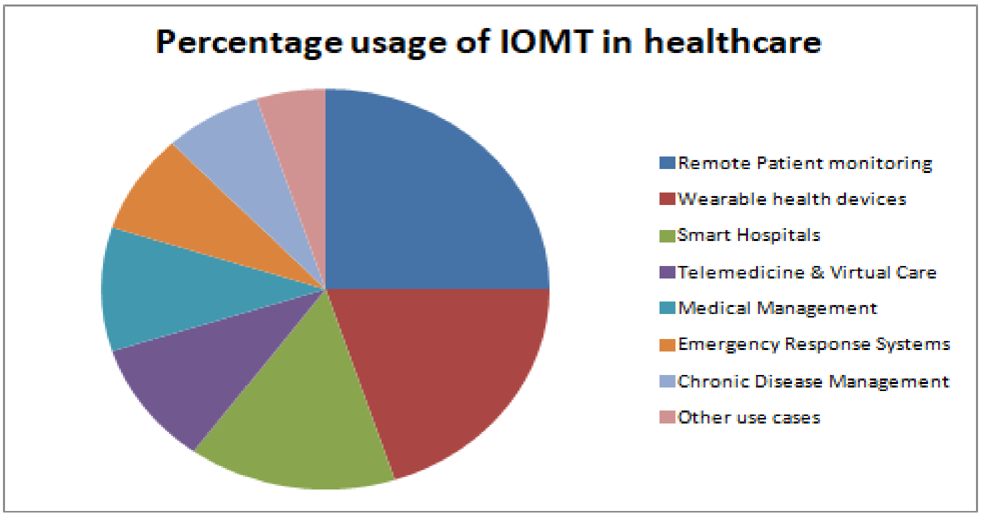

Fig. 2. Percentage usage of IOMT in Healthcare.

2.3.1 Remote patient monitoring

Remote Patient Monitoring (RPM) using the Internet of Medical Things (IoMT) enables continuous healthcare outside traditional hospital settings by integrating smart medical devices, cloud computing, AI, and secure data transmission. The RPM process follows six stages: data acquisition via IoMT sensors, wireless transmission through 5G and Bluetooth, cloud-based storage and AI-driven analysis, real-time health assessment, automated alerts and telemedicine integration, and continuous monitoring with predictive analytics. Key components include IoMT sensors, edge computing, AI-driven diagnostics, blockchain for security, and early warning systems. However, challenges such as interoperability, data security, energy efficiency, and regulatory compliance persist. Future research focuses on integrating blockchain for secure data sharing, AI-driven triage, 5G for low-latency transmission, and Explainable AI (XAI) for better clinical decision-making [19] [20].

2.3.2 Smart wearables and implantable devices

Smart wearables and implantable devices are transforming healthcare through the Internet of Medical Things (IoMT), enabling real-time, continuous patient monitoring. Wearables such as ECG monitors, Smartwatches, and biomedical clothing track vital health metrics, aid in chronic disease management, and leverage AI for early disease detection. Implantable medical devices, including pacemakers, seizure detectors, and glucose monitors, provide automated therapeutic interventions and remote monitoring capabilities. Despite their potential, challenges such as data security, interoperability, battery life, and AI accuracy hinder widespread adoption. Future advancements in blockchain security, energy harvesting, and AI-driven analytics will further enhance personalized and predictive healthcare solutions [21] [22] [23].

2.3.3 P4 Medicine (Predictive, Preventive, Personalized, Participatory)

P4 Medicine Predictive, Preventive, Personalized, and Participatory leverages the Internet of Medical Things (IoMT) to revolutionize healthcare by integrating AI, multimodal data fusion, and real-time monitoring. Predictive medicine uses AI and wearable devices to foresee diseases like epilepsy and cardiovascular disorders, enabling early intervention. Preventive medicine employs continuous tracking through smart wearables to detect health risks, while blockchain enhances data security. Personalized medicine tailors' treatments using genomics and sensor-based data to optimize drug delivery and precision oncology. Participatory medicine empowers patients through mHealth apps, telehealth, and AI-driven coaching for active healthcare engagement. Together, these advancements transform healthcare into a proactive, data-driven, and patient-centric model [24], [25].

2.3.4 Disease diagnosis and management through IoMT

The Internet of Medical Things (IoMT) disrupts the diagnosis and management of diseases because it is going to connect medical devices, AI-based analytics, and cloud computing to augment healthcare performance. The architecture is composed of sensor layer, network layer and application layer, and it supports real time data collection, secure wireless transmission and AI-based diagnosis. Applications of IoMT enable early diagnosis of diseases including CT scan analysed brain hemorrhage and prediction of heart diseases with AI models. It also helps in chronic disease management, remote patient monitoring, and automated treatment adjustments. Nevertheless, issues such as data security, interoperability, and computational constraints need to be resolved by evolving emerging blockchain, standardisation, and AI optimization in order to exploit the potential of IoMT for personalized healthcare [26] [27].

2.3.5 Telemedicine & virtual care

"Telemedicine and Virtual Care are the two interconnected IOMT applications that are even transforming health care by providing the remote diagnosis, monitoring, consultation etc. through networking medical devices. This cybernetic network allows continuous data reading from implanted devices and wearable sensors in the form of real-time data sent from cloud-connected devices to healthcare professionals. This improves telemedicine through timely interventions and personalized treatment. In virtual health, the IoMT enables remote patient monitoring (RPM) via continuous monitoring of vital signs, eliminating the need for visits to the hospital, and increased access for people in remote locations. In addition, AI-powered data fusion approaches can improve diagnostic accuracy by combining heterogeneous sensor data together, which is beneficial for better delivery of health care. Yet, the issues of data security, interoperability, and network accessibility must be solved to fully tap into the potential of IoMT in telemedicine and virtual care [28][18].

2.3.6 Emergency Response Systems

IoMT as an essential enabler for emergency response systems with features including real-time parent monitoring, MF-driven analytics and networked medical devices. Through the IoMT, data can be more quickly transferred from ambulances to hospitals, as emergency patients can be continuously tracked via wearable biosensors and medical imaging equipment. Lightning-Fast 5G and Small Cell Networks Medical video streaming for remote diagnosis and timeline intervention benefit from high-speed 5G and small-cell networks. AI-based event detection, in conjunction with cloud and fog computing, provides automated emergency alerts and prediction descriptions that would minimize response times. Furthermore, robotic ambulance systems and telemedicine platforms based on the Internet of Medical Things (IoMT) enhance pre-hospital care, leading to decrease mortality in life-threatening circumstances as in the case of cardiac arrest. However, the paper also discusses issues such as network latency, data security, and inter-operability, which highlights the requirement of reliable, scalable, and privacy-preserving IoMT Systems for emergency healthcare applications [29][78].

2.3.7 Smart Ambulances

Smart ambulance using the Internet of Medical Things (IoMT) as an emergent concept in the emergency medical services. IoMT integrated smart ambulances are designed with real-time patient monitoring, AI-based diagnostics, and cloud-based data analytics for improved pre-hospital care. Wearable and implantable medical devices monitor patients' vital signs around the clock – including heart rate, blood pressure, oxygen levels and ECG data – and send wireless updates over 5G-connected networks to hospital systems, enabling emergency physicians to prepare themselves before the patient arrives. The edge and fog architectures are used to analyse data at the local level and limit latency with on-the-spot decision-making. AI-driven predictive analytics also help to triage patients and to improve ambulance routes. Blockchain and encryption technologies provide security for privacy of medical data transmission. Nevertheless, for larger adoption a number of issues, such as interoperability, cybersecurity problems, and substantial infrastructure costs, have to be solved. The incorporation of IoMT in smart ambulances would benefit patient outcomes by decreasing response time and early medical management [30].

2.3.8 Smart Surgical Instruments

Smart Surgical Instruments as an exemplary instance of the Internet of Medical Things (IoMT) improving precision, efficiency, and real-time decision-making during a surgery. This new generation of smart surgical tools empowered by IoMT combines AI, robotics and real-time data analytics to enable surgeons to probe inside patients with extreme precision and responsiveness. The devices have built-in sensors and/or actuators and are also capable of wireless communication for remote monitoring and/or tele-surgery. AI-powered feedback systems are used to examine surgical data in real-time for error detection and decision support during the surgery. Additionally, cloud and edge computing support data analysis and processing to enhance the quality of surgery by the use of predictive analytics and/or machine learning models. But the paper also identifies standing problems like data safety and real-time processing latency, proxy to strong network assurance to move things closer to safe IoMT acquiesced surgeries. Resolution of such problems will facilitate in robotic assisted surgery, personalised medicine, and postoperative observations to enhance patient's safety and surgery success [31].

2.3.9 Connected Contact Lenses.

Connected Contact Lenses as a sophisticated IoMT application for real-time health monitoring and diagnostics. These intelligent lens systems combine biosensors, wireless communication, and artificial intelligence for real-time analysis of physiological parameters including glucose, intraocular pressure, and tear composition, which will be of great value to diabetic and glaucoma patients. Coupled with 5G networks and edge computing, these lenses give doctors the ability to receive instantaneous health data from a patient, thereby facilitating disease detection at an early stage and remote patient monitoring. AI-driven data analysis improves predictive analytics by providing information on the progression of a disease and treatment response. But the paper notes that such devices face obstacles, including data security, scaling-down electronic components to sizes that can comfortably enter the body, and the efficiency of the devices. Solving such issues can pave the way to potential breakthroughs in personalized medicine and telemedicine, facilitating easier and simultaneous non-invasive, continuous monitoring of overall health status [32][12].

3 Challenges in IoMT

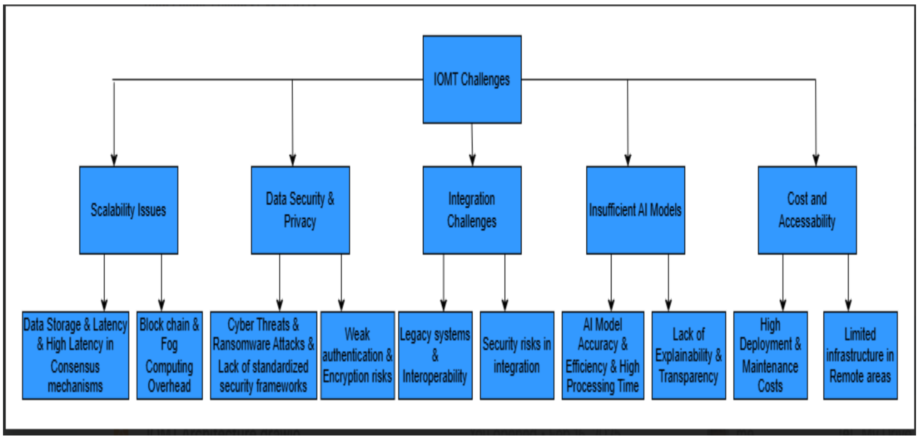
IOMT Challenges
Scalability Issues
Data Security & Privacy
Integration Challenges
Insufficient AI Models
Cost and Accessability
Data Storage & Latency & High Latency in Consensus mechanisms
Block chain & Fog Computing Overhead
Cyber Threats & Ransomware Attacks & Lack of standardized security frameworks
Weak authentication & Encryption risks
Legacy systems & Interoperability
Security risks in integration
AI Model Accuracy & Efficiency & High Processing Time
Lack of Explainability & Transparency
High Deployment & Maintenance Costs
Limited infrastructure in Remote areas

Fig. 3. Categorization of Key Challenges in IoMT Adoption and Implementation.

The paper structure is illustrated by the given diagram in Fig 3, which aims to provide a comprehensive view of the main challenges of IoMT. Loosely abstracted, the identified challenges can be classified at its top-level into five main challenge domains: Scalability Challenges, Data Security & Privacy, Integration Challenges, Inadequate AI Models, and Cost & Accessibility. Each of these areas is divided into subcategories within which challenges preventing successful IoMT adoption and use are given emphasis. Issues of scalability result from limited storage of data, consensus latency and the computational burden incurred by blockchain and fog computing. All these sources of threats including cyber risks, Ransomware threats, poor authentication and non-existence of common security frameworks that are essential to maintain the confidentiality of patients' data and operability of a system.

Besides, integration challenges involve interoperability between traditional e-healthcare systems and current IoMT platforms and security threats during system integration. The figure also highlights why the role AI technology can play in IoMT is limited with the potential for high processing efforts, inefficiencies, and a lack of explainability of in AI-based decision-making integration in clinical use. Finally, issues on cost and accessibility indicate economic barriers, which involve high installation and operational costs as well as limited infrastructure in remote areas. To overcome these challenges, technological advances, regulatory framework, synergy, and continued efforts are essential to drive the scalability, security, interoperability, AI optimization, and cost-effective deployment for equitable healthcare access of the IoMT.

3.1 Scalability Issues

In large-scale deployments of IoMT systems, scalability concerns are related to data storage, network latency, interoperability, energy consumption, and security. The massive amount of the real-time medial data generated by IoMT devices (devices of IoMT) overwhelms storage and computing resource, especially for the crowded mass of adding blockchain and fog computing technologies. The latencies are high using consensus mechanisms such as Proof-of-Work discarding the real-time property and the absence of uniform protocols creates barrier in integrating a device uniformly in both cloud and edge. The energy efficiency is also an issue, as energy constrained IoMT devices are struggling to satisfy the power requirement of the blockchain networks [33] [34]. Furthermore, the increase in the scale of IoMT networks contributes to the growth of cyber security threats, which in turn leads to off-chain storage and encryption mechanisms, thus incurring computational overheads. The aforementioned scalability issues will need to be addressed for the IoMT to reach its full potential and to fully harness the proliferation of the devices mentioned previously with the advancements around efficient data management, alternative consensus models, and energy-efficient security models which can work to achieve balance between performance, reliability, and security of large-scale adventure of the IoMT future [35][16].

3.2 Data Security and Privacy Concerns

The Internet of Medical Things (IoMT) is an essential aspect for enhancing healthcare systems through collecting real-time data, but poses serious security and privacy issues such as: cyber threats, intruder access, data mining and Ransomware. Patient data is left vulnerable to potential malicious threats due to poor authentication and encryption methods, which could result in data breaches, impersonation, or device tampering. The security measures available in IoMT are challenged in terms of standardization, intrusion detection, and obeying the laws and regulations [37] [38]. Novel methods for securing the process may be those that are tamper proof, such as Blockchain, AI based anomaly detection, multi-factorial authentication, lightweight crypto and others, however some of the methods offer not yet proved solutions. Nevertheless, enforcement of regulations and adoption of formal security standards is required to protect patient data and enable secure medical device operations [39] [40] [88].

3.3 Integration Challenges

Adoption of IoMTs is cumbersome as incorporation with existing healthcare systems and into vendor specific platforms become problematic around interoperability, security, scalability constraints, and absence of regulatory compliance. Many legacy systems do not have the use of standardized communication protocols, resulting in actualize their compatibility with newer IoMT devices challenging. Security issues like legacy encryption and cyber-threats, make integration even more challenging [41] [42] [43]. Further, the wide variety of vendors with proprietary data formats and communication technologies leads to fragmentation, with increased expense and decreased efficiency in healthcare. Standardisation activities, blockchain for data security, federated identity management; and cloud-based integration solutions have started exploring as methods to overcome these challenges and propagate the adoption of IoMT [44] [45].

3.4 Insufficient AI Models

Limited AI models in the Internet of Medical Things (IoMT) are faced with real-time data processing, efficiency and interpretability difficulties. Real-time AI/ML models are critical for applications such as intensive care monitoring and seizure detection, but face challenges including large data volumes, end-to-end latency sensitivity, and federated learning delays. Possible solutions include edge computing, federated learning, and data compression. Lightweight AI/ML models are also vital since IoMT devices are resource-constrained and need low-complexity algorithms or hybrid techniques for effectiveness [46] [47]. Moreover, the so-called black box of decisions made in healthcare with AI, it's transparent, reliable, but which will need to comply with regulations, trust and transparency. More complex AI models tend to be “black boxes”, which can hinder clinicians' ability to understand their findings. Explainable AI techniques, for example, SHAP, LIME, human-in-the-loop (HITL) approaches might improve interpretability to maintain a accountable and trustworthy AI adoptions in IoMT. In the future, it is hoped that more work will be done to optimise models for efficiency and security, interoperability and a better understanding of AI and provide an opportunity to enhance the trust in AI-driven healthcare [48] [49] [50][11].

3.5 Cost and Accessibility

Limitations The current cost and accessibility of Internet of Medical Things (IoMT) solutions may be a barrier to broad adoption, particularly in low-resource settings. Deployment costs originate from infrastructure like advanced sensors, edge computing, cloud integration, as well as cyber security investments and high-performance computing [51]. Moreover, it is rather challenging to go to remote places that suffer from lack of network, unreliable power supply, and expensive IoMT devices and maintenance. Add a shortage of trained professionals, lack of awareness, regulation complexity and cyber security concerns to inhibit adoption. Addressing these challenges calls to cost-effective IoMT solutions, enhanced infrastructure of IT, government aid, and customized regulatory frameworks to ensure fair healthcare access [52].

4 Challenges in IoMT Adoption

Despite its potential, the deployment of IoMT is facing the hurdles of security Data risks, interoperability problems and regulatory compliance. Data security is essential due to cyber threats and concerns about privacy, and a lack of standardization is a barrier for the integration of the device in a day to day. What’s more, high implementation cost and apprehension regarding new technology act as barriers to healthcare uptake.

4.1 Technical Challenges of IoMT

IoMT is offering a revolution in healthcare and has potential to provide for patients’ real-time monitoring, diagnostics at a distance, and automatic medical processes. But there are significant obstacles of network latency, bandwidth and device reliability, and lifecycle management to get it widely deployed. These issues must be overcome to provide high quality and efficient health care [53].

Network latency describes the time delay of the data send between IoMT devices and central processing units, which is essential for real-time applications, such as remote surgery and emergency calls. To reduce the response time, technologies like 5G and Mobile Edge Computing (MEC) are employed to work on the data closer to the devices than having to communicate over the network with a distance cloud server only. Bandwidth constrains from the amount of data generated by the IoMT devices are also an obstacle. Apps such as telemedicine and AR surgical assist need high bandwidth low latency networks. Approaches like edge computing that locally analyse data are useful in saving bandwidth, whereas protocols like NB-IoT or LoRaWAN support long distance connectivity for non-real-time health monitoring [54].

Reliability of the device is important for patient safety and appropriate healthcare delivery. IoMT devices encounter opportunities and challenges on hardware failures, sensor moderations, cyber threats such as ransoms, and the incompatible problem. Reliable and accurate data collection is vital as the use of erroneous sensor reading could result in patients receiving incorrect medical care. Moreover, reliability of devices may be impaired by security threats such as unauthorized access and hacker attacks. To facilitate interoperability among IoMT devices, it is also important to standardize communication protocol [55].

Lifecycle management of IoMT systems include updating software, performing maintenance, remaining compliant with regulations and being able to still connect. Often, these IoT medical devices do not provide remote upgrade functionality and can become outdated and insecure. Further, maintenance and scalability are complicated by the increasing number of connected devices. Laws on ownership of data, privacy, and ethics make lifecycle management even more challenging. Compliance to healthcare regulations and investment in remote software update, encryption algorithms, and secure data management provide opportunities for prolonging the life span of IoMTs [56]. Fig. 4 shows the Technical Challenges.

In summary, addressing networking and device issues remains central to the success and growth of IoMT. The incorporation of 5G, MEC, cyber security frameworks and scalable device management solution will enhance efficiency and reliability. It is imperative for new healthcare industry players like manufacturers, regulators, and healthcare providers to work together when building a secure and sustainable IoMT ecosystem that improves patient care [57] [58].

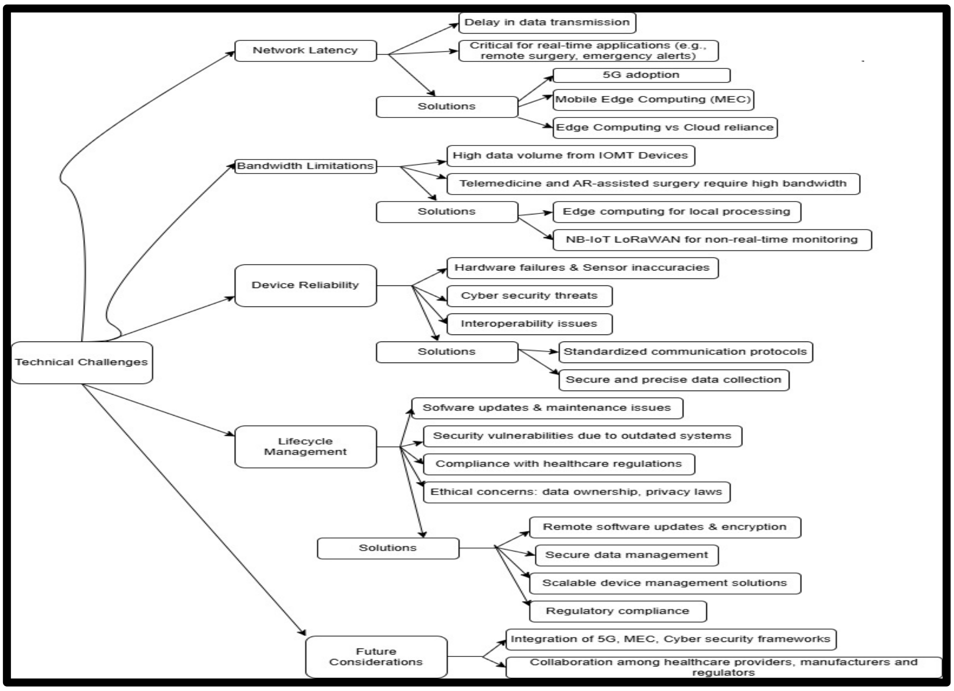
Technical Challenges
Network Latency
Delay in data transmission
Critical for real-time applications (e.g., remote surgery, emergency alerts)
Solutions
5G adoption
Mobile Edge Computing (MEC)
Edge Computing vs Cloud reliance
Bandwidth Limitations
High data volume from IOMT Devices
Telemedicine and AR-assisted surgery require high bandwidth
Solutions
Edge computing for local processing
NB-IoT LoRaWAN for non-real-time monitoring
Device Reliability
Hardware failures & Sensor inaccuracies
Cyber security threats
Interoperability issues
Solutions
Standardized communication protocols
Secure and precise data collection
Lifecycle Management
Sofware updates & maintenance issues
Security vulnerabilities due to outdated systems
Compliance with healthcare regulations
Ethical concerns: data ownership, privacy laws
Solutions
Remote software updates & encryption
Secure data management
Scalable device management solutions
Regulatory compliance
Future Considerations
Integration of 5G, MEC, Cyber security frameworks
Collaboration among healthcare providers, manufacturers and regulators

Fig. 4. Technical Challenges.

4.2 Regulatory and Ethical Concerns

The Internet of Medical Things (IoMT) faces significant regulatory challenges due to the lack of standardized global regulations. The absence of universal security, interoperability, and data privacy standards across healthcare systems hinders seamless communication among devices and infrastructures. Interoperability issues arise as IoMT devices from different manufacturers use varying protocols, leading to fragmentation and inefficiencies in healthcare operations [59] [60]. Additionally, inconsistencies in data security regulations expose patient information to breaches and cyber threats. Although organizations like the FDA and HIPAA have introduced regulations, there is no unified global framework, making compliance difficult for IoMT manufacturers. These regulatory gaps also create ethical and legal concerns, such as unclear policies on patient consent, data ownership, and AI usage. Without clear guidelines, IoMT adoption faces delays, reducing trust among healthcare providers and patients. To mitigate these challenges, experts propose developing global security and privacy standards, unified interoperability guidelines, and stronger legal frameworks to govern IoMT devices [61] [62]. Fig. 5 shows the Regulatory and Ethical Concerns.

AI and data usage in healthcare and IoT systems raise several ethical dilemmas, particularly in privacy, bias, transparency, and accountability. AI-driven systems collect large volumes of sensitive personal data, increasing concerns about security, unauthorized access, and potential misuse. Techniques like blockchain and anonymization can help protect data, but they pose implementation challenges. Algorithmic bias is another issue, as AI models trained on historical data may reinforce unfair treatment, especially in healthcare. Ensuring transparency is also crucial, as many AI models function as "black boxes" with unclear decision-making processes. Additionally, AI-driven recommendations can manipulate user behavior, affecting autonomy and ethical integrity. In healthcare, AI must be designed to provide unbiased diagnostics and treatment recommendations while ensuring data ownership and patient control. Legal frameworks and governance models are necessary to define accountability, particularly for incorrect diagnoses or biased AI decisions. Addressing these ethical challenges requires regulatory oversight, transparency measures, and fairness-driven AI policies, with blockchain offering potential solutions despite its own challenges [63] [64].

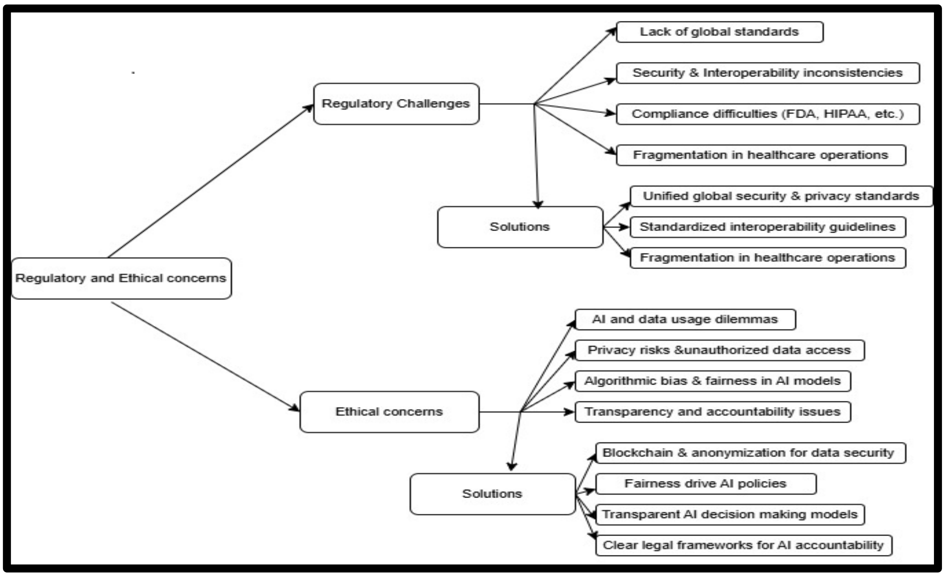
Regulatory and Ethical concerns
Regulatory Challenges
Lack of global standards
Security & Interoperability inconsistencies
Compliance difficulties (FDA, HIPAA, etc.)
Fragmentation in healthcare operations
Solutions
Unified global security & privacy standards
Standardized interoperability guidelines
Fragmentation in healthcare operations
Ethical concerns
AI and data usage dilemmas
Privacy risks &unauthorized data access
Algorithmic bias & fairness in AI models
Transparency and accountability issues
Solutions
Blockchain & anonymization for data security
Fairness drive AI policies
Transparent AI decision making models
Clear legal frameworks for AI accountability

Fig. 5. Regulatory and Ethical Concerns.

4.3 User Acceptance

Adoption of the Internet of Medical Things (IoMT) for healthcare is somewhat resisted by professionals and patients, being preoccupied with technology complexity, security, interoperability and ethical issues. Practitioners grapple with training voids, problems with interoperation, and the dependability of IoMTs, concerned that malfunctions can result in catastrophic medical mistakes. In addition, tough privacy laws and fears over cyber security make them reluctant. From the patient perspective, trust concerns and consent, the fear of over-surveillance, and digital literacy challenges present barriers to the adoption of IoMT solutions. Tackling these issues will involve better training, consistent device protocols, strong security practices, transparent patient involvement, and better infrastructure to enable the use of IoMT [65]. Fig. 6 shows the User Acceptance.

One critical requirement for successful IoMT acceptance is the user-friendly interface that facilitates the use of the technology for both healthcare professionals and patients. User-friendly applications with real-time monitoring, decision-support facilities and smooth interoperability \can increment healthcare efficiency, and do so while fulfilling security and privacy. By using blockchain-based authentication, encryption, and common protocols, the stakeholders can collectively solve these integration and security challenges. Applications that also provide simple data visualization, give alerts, report on remote access can go a long way in gaining patient confidence and attention. Future work should aim to develop easy-to-use, secure, and established IoMT apps with usability and realistic innovation that enhances patient outcome and ease of health care access [66] [67].

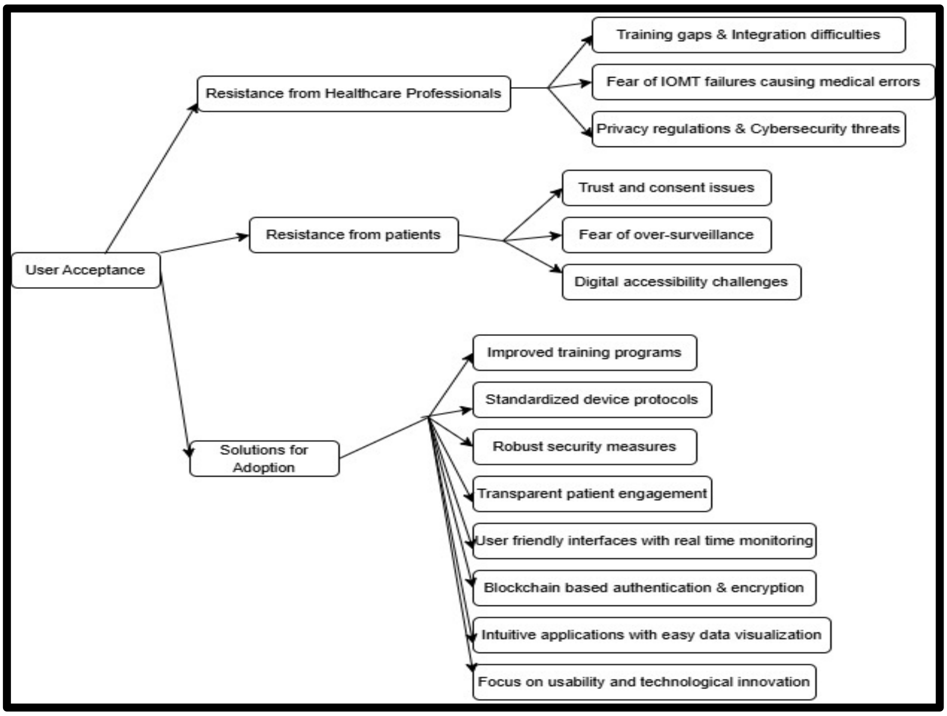
User Acceptance
Resistance from Healthcare Professionals
Training gaps & Integration difficulties
Fear of IOMT failures causing medical errors
Privacy regulations & Cybersecurity threats
Resistance from patients
Trust and consent issues
Fear of over-surveillance
Digital accessibility challenges
Solutions for Adoption
Improved training programs
Standardized device protocols
Robust security measures
Transparent patient engagement
User friendly interfaces with real time monitoring
Blockchain based authentication & encryption
Intuitive applications with easy data visualization
Focus on usability and technological innovation

Fig. 6. User Acceptance.

5 Emerging Trends and Future Research Directions

Emerging trends in IoMT include AI-driven diagnostics, blockchain for data security, 5G-enabled remote healthcare, and edge computing for real-time processing. Future research focuses on enhancing interoperability, cybersecurity, and personalized medicine. Advancements in wearable technology and predictive analytics will further revolutionize healthcare delivery.

5.1 Advancing AI and ML for IoMT

Advancing AI and ML in IoMT enables real-time monitoring, predictive analytics, and automated decision-making in healthcare. Explainable AI (XAI) enhances trust, while Federated Learning (FL) ensures data privacy by decentralizing AI training. Integrating blockchain improves security, and future research focuses on optimizing AI for scalability, efficiency, and interoperability in IoMT systems [79].

5.1.1 Explainable AI (XAI) for Trustable Decision-Making

XAI in IoMT increases trust, transparency as well as interpretability of AI in health care. This will also serve to mitigate the “black-box” nature of AI by providing interpretable predictions and adherence to clinical standards. Approaches such as SHAP and LIME advance interpretability, while XAI also promotes security through bias and anomaly detection in medico data. However, the dichotomy between interpretability and diagnostic performance must be balanced, and there is an issue with regard to the computational power of IoMT devices. In addition, further studies can be conducted on light-weight and real-time xai model, and make the framework standardized for popularization in health care. [68] [69] [70] [71] [81][73].

5.1.2 Federated Learning for Data Privacy in IoMT

The IoMT transforms healthcare through real-time monitoring and spread diagnostics; nevertheless, it brings about new privacy issues. Federated Learning (FL) is a step in the right for direction as it allows to decentralize training of AI models, so that data can be private and yet collaborate on building a global model. Security is improved with approaches such as Differential Privacy, Homomorphic Encryption, and Secure Multiparty Computation. Adding blockchain to the solution along with FL escalation the system security and data transparency. Yet, issues such as communication overhead and resource constraints remain. In future studies, it would be very interesting to investigate the optimization of FL and XAI for scalable, privacy-preserving and real-time healthcare applications [72] [76] [77].

5.2 Enhancing Security and Privacy Mechanisms

Improved security and privacy measures are important for securing sensitive medical information from cyber threats in IoMT. Privacy-enhancing technologies namely Federated Learning (FL), Differential Privacy (DPM), Homomorphic Encryption (HE), and Blockchain guarantee a secure data processing and storage. Improving the robustness of encryption, authentication, and anomaly detection is necessary to improve privacy confidence and trust levels within the context of IoMT systems.

5.2.1 Implementing Blockchain for Secure IoMT Networks

Blockchain in IoMT improves data integrity, security, and interoperability by offering a decentralized immutable distributed ledger that prevents unauthorized access and modification of data. Smart contracts automatically manage access control and enforce privacy rules. Methodologies like B-IAKE and BlendCAC enhance authentication and access control and the implementation of blockchain into fog and edge computing optimizes resource utilization. Blockchain ensures that risks such as MitM attacks and data integrity are minimized, through encryption and decentralized identity management. Applications can be found in EHR management, remote patient monitoring, and pharmaceutical authentication, but challenges of scaling and machine learning integration require more investigation 7476.

5.2.2 Developing Advanced Encryption Techniques for IoMT Security

Advanced encryption is a key factor for IoMT security as IoMT carries sensitive medical data and these devices have limitations. Light-weight cryptographic mechanisms such as optimized AES, ABE, and hybrid encryption for secure key exchange are also being considered for study 78. Proven Data Possession (PDP)- and smart contracts-based encryption also achieve secure sharing and integrity in the blockchain (fast and in a fine-grained way: Secured Proven POS). Security cannot be left out when it comes to AI, as it enhances encryption with dynamic cryptography model and anomaly detection and supports secure communication based on federated learning. Recently, new approaches such as homomorphic encryption, crypto-stegno, multi-factor authentication (MFA) have enhanced the security of networked data. Next-generation research should centre on quantum-secure encryption, AI-powered protection of keys, and zero-trust architectures for bolstering security and regulatory compliant adherence among IoMTs [80] [15].

5.3 Energy-Efficient and Sustainable IoMT Systems

Energy-efficient and green IoMT systems are geared at low energy consumption with reliable healthcare monitoring. Methods such as low power communication (e.g., BLE, Zigbee, 5G), edge computing, and adaptive power management contribute to minimizing an energy utilization. Attachment of renewable sources of energy and energy-efficient AI models adds to sustainability. Next developments will focus on the green IoMT solutions for long-term efficiency.

5.3.1 Designing Low-Power IoMT Devices for Longer Operational Lifespans

It is important to develop low-power IoMT devices, since such devices must have long operational lifetimes in energy-efficient manner. Clustering methods including the Fuzzy Logic-Based Clustering (FC-IoMT) limit energy consumption in a manner of data transmission. Both are what could be considered edge and fog computing, which reduces reliance on the cloud and power usage. Energy conserving protocols such as BLE, ZigBee, and optimized Wi-Fi also further contribute towards efficiency. On the other hand, the nanogenerators for energy harvesting technique are a potential low-carbon power solution, while the wireless charging is confronted with numerous issues. Next generation improvements will incorporate power-efficient biosensors and adaptive machine learning for enhanced real-time monitoring [82] [83].

5.3.2 Energy Harvesting and Algorithmic Optimization for IoMT

Energy recapturing methods, such as mechanical transformation, wireless charging, and bio-energy scavenging, have been proposed to maintain the IoMT device function. AI based models are employed to manage power by predicting transmission requirements and lightweight cryptographic solutions are also available to provide security while minimizing the energy utilization [84].

5.3.3 Integration of Renewable Energy for Sustainable IoMT Healthcare

The use of RES such as solar, wind, and hydropower combined with IoMT supports sustainability and reliability, particularly in remote locations. These stand-alone power plants are characterized by battery energy storage (BESS) and hybrid renewable energy systems (HRES) for uninterrupted power. The grid smart, AI-support energy management allows for efficient power distribution and consumption. There are challenges to be faced in terms of energy intermittency, infrastructure constraints, and cybersecurity exposure. Research directions Interest targets on potential topics for further research should in fact be focused on advancement of energy storage technologies, AI-enabled optimization, secure renewable-powered IoMT systems that could ensure resilience in healthcare [85][17].

5.4 Standardization and Interoperability

Standardization and interoperability in the IoMT allow medical devices and healthcare systems to communicate with each other without encountering any issues. HL7, FHIR, IEEE 11073 etc., are some frameworks that allow for efficient data exchange and to monitor, in real-time. Overcoming the data silos, security concerns and regulatory issues is essential for the mass adoption. Unified standards and secure IoMT interoperable mechanisms would promote the indexed, advanced and personalized patient care.

5.4.1 Establishing Global IoMT Standards for Seamless Integration

The standardization of IoMT, therefore, is key for smooth and secure integration of devices and their interoperability in healthcare systems. The absence of universal standards, meanwhile, poses a problem making different technology-using gadgets, such as Wi-Fi, Bluetooth and LTE, all talk to each other. HIPAA and GDPR compliance inherently complicate the approach due to secure data exchange. Moving to an FHIR, IEEE 802.15.6, blockchain and AI enabled analytics-based platform solutions may enable better interoperability and security in terms of data protection. Future work could explore AI-based middleware, quantum cryptography, and worldwide policies for the global IoMT to promote a secure and efficient healthcare system [86].

5.4.2 Developing Frameworks to Enhance Cross-Platform Compatibility

Interoperability of the IoMT across platforms is difficult as there are various devices, operating systems and communication protocols. These ‘Fog-Cloud Architecture Based IoMT’ standardized frameworks combine heterogeneous systems to achieve cost effective real-time and cloud-based processing. Security is addressed through the use of blockchain, encoding schemes and cryptographic hashing to guarantee the integrity of data. AI and ML enable improved integration of IoMT data, which will help with decision support and anomaly detection as it relates to malware threats. The process is multi-faceted and spans a series of activity layers, securing incisive data types effectively and obtaining regulatory approval from healthcare data [87][75].

5.5 Socio-Economic Considerations

Socioeconomic concerns of IoMT are affordability and accessibility and digital health equity of care. High cost of implementation and infrastructure gaps may restrict scale-up, particularly in low-resource settings. Strategies such as cost-effectiveness guarantee, digital gap crossing and ethical concerns have to be felt, to maximize the potential of IoMT for every population.

5.5.1 Addressing Disparities in IoMT Accessibility Across Geographies

Infrastructure barriers, economic constraints, and interoperability issues, particularly in settings of low- and middle-income countries (LMICs) impede access to IoMT. Challenges such as network availability, high installation cost, and lack of skilled personnel constrain the uptake. Scaling telemedicine, using AI as well as blockchain for security and investing in digital infrastructure such as 5G could narrow the divide. An integrated interventional policy, funding and technological rely initiative is essential for the equitable deployment of IoMT.

5.5.2 Strategies to Reduce Costs without Compromising Functionality

Minimizing the deployment cost of the IoMT without compromising its efficiency involves intelligent use of cloud and edge computing, optimizing the storage and processing. Standardisation, and open-source platforms brings down the cost of development and improves interoperability. Predictive maintenance by AI minimises machine shut down so that machines can continue to produce at any time; LPWANs like NB-IoT also offer highly economical connections. Authentication and data management are simplified via blockchain, with infrastructure costs reduced. Energy-efficient devices and telemonitoring systems lead to additional financial savings by prolonging battery life and reducing hospital visits. Scalable and affordable with cloud-based frameworks and subscription-based models for IoMT adoption.

6 Future Directions

AI, security, energy efficiency, standardization, and accessibility as the five aspects that are driving the future of IoMT. Key research areas include:

AI and ML Optimisation for IoMT Future work will further optimize the Explainable AI (XAI) models to make real-time, trustable decisions with still-computationally efficient methods. Improvement of FL, will mitigate the problem of communication overhead as well as scalability to guarantee secure privacy reserving AI training.

Enhancing Security and Privacy: The focus will be on quantum-resistant encryption, zero trust architectures and AI-based anomaly detection for protecting IoMT networks. The use of blockchain-based federated learning will enable data protection and compliance with future regulations.

Sustainable and Energy-Efficient IoMT: Energy harvesting (nanogenerators, bio-energy conversion) technology will enhance the sustainability of devices. AI-guided power optimization algorithms will help lower energy consumption, extend equipment life- cycle.

Strengthening the Interoperability and Standardization: Universal global standards and AI based middleware solution is needed to enable free communication across platforms. Quantum cryptography and secure APIs are used to achieve interplay between a variety of IoMT ecosystems.

Fostering Inexpensive and Equitable IoMT Technologies: Upcoming efforts will focus on affordable deployment techniques (e.g., cloud-edge hybrid architectures), and open-source frameworks. Across the health facilities operating in low resource settings, their current lack of telecommunication infrastructure coupled with recent findings that IoMT was well accepted in these settings, necessitates that we begin building a 5G and digital infrastructure.

7 Conclusion

The Other Side of Medical IOT: The Internet of Medical Things (IoMT) is transforming the healthcare in a new light- caring the patients better, making operations efficient and, lowering the burdening costs. IoMT is a system consisting of interconnected devices, wearables, and sensors that can gather, transmit, and assess real-time health data. we will get the pros such as Remote patient monitoring (RPM), Telemedicine report, early disease detection, Operational efficiency, improve patient safety, reduce cost. Although IoMT is promising, obstacles such as data security, system interface, and regulatory requirements need to be considered. It may be said that hereafter, with the development of technologies such as AI and 5G, IoMT will define the prospects of personalized / preventive medicine. IoMT is transforming medical care, providing improved medical results and cost savings. But risk and interoperability, infrastructure, device reliability, and ethical considerations must be considered for growth to be sustainable. Leveraging AI, blockchain, 5G and robust regulations, IoMT can become a trustable and scalable healthcare technology. It is also transforming the healthcare system as well as global healthcare as a whole, both in terms of accessibility as well as the quality of healthcare services. Its influence is not limited to technological advancement but also to developing a patient-centric, data-driven, and cost-effective healthcare system. IoMT is a linchpin for the forthcoming digital healthcare revolution that is delivering a more equitable, efficient and data-driven global health ecosystem. Though issues around security, interoperability, and infrastructure to be solved, the potential payoffs in the long-run in terms of patient outcomes, cost savings, and healthcare access make IoMT an unalloyed positive force shaping medicine in the 21st century.

References

[1] Khan, N. A., Awang, A., & Karim, S. A. A. (2022). Security in Internet of Things: A Review. IEEE Access, 10, 104649–104670. https://doi.org/10.1109/access.2022.3209355.

[2] Pradyumna, G. R., Hegde, R. B., Bommegowda, K. B., Jan, T., & Naik, G. R. (2024). Empowering Healthcare with IoMT: Evolution, Machine Learning Integration, Security, and Interoperability Challenges. IEEE Access, 12, 20603–20623. https://doi.org/10.1109/access.2024.3362239.

[3] Mahmood, M., Khan, M. I., Ziauddin, Hussain, H., Khan, I., Rahman, S., Shabir, M., & Niazi, B. (2023). Improving Security Architecture of Internet of Medical Things: A Systematic Literature Review. IEEE Access, 11, 107725–107753. https://doi.org/10.1109/access.2023.3281655.

[4] Messinis, S., Temenos, N., Protonotarios, N. E., Rallis, I., Kalogeras, D., & Doulamis, N. (2024). Enhancing Internet of Medical Things security with artificial intelligence: A comprehensive review. Computers in Biology and Medicine, 170, 108036. https://doi.org/10.1016/j.compbiomed.2024.108036.

[5] Huang, C., Wang, J., Wang, S., & Zhang, Y. (2023). Internet of medical things: A systematic review. Neurocomputing, 557, 126719. https://doi.org/10.1016/j.neucom.2023.126719.

[6] Rathore, M. M., Shah, S. A., Shukla, D., Bentafat, E., & Bakiras, S. (2021). The Role of AI, Machine Learning, and Big Data in Digital Twinning: A Systematic Literature Review, Challenges, and Opportunities. IEEE Access, 9, 32030–32052. https://doi.org/10.1109/access.2021.3060863.

[7] Malamas, V., Chantzis, F., Dasaklis, T. K., Stergiopoulos, G., Kotzanikolaou, P., & Douligeris, C. (2021). Risk Assessment Methodologies for the Internet of Medical Things: A Survey and Comparative Appraisal. IEEE Access, 9, 40049–40075. https://doi.org/10.1109/access.2021.3064682.

[8] Mathkor, D. M., Mathkor, N., Bassfar, Z., Bantun, F., Slama, P., Ahmad, F., & Haque, S. (2024). Multirole of the internet of medical things (IoMT) in biomedical systems for managing smart healthcare systems: An overview of current and future innovative trends. Journal of Infection and Public Health, 17(4), 559–572. https://doi.org/10.1016/j.jiph.2024.01.013.

[9] Ahmed, S. F., Alam, Md. S. B., Afrin, S., Rafa, S. J., Rafa, N., & Gandomi, A. H. (2024). Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions. Information Fusion, 102, 102060. https://doi.org/10.1016/j.inffus.2023.102060.

[10] Sai, S., Bhandari, K. S., Nawal, A., Chamola, V., & Sikdar, B. (2024). An IoMT-Based Incremental Learning Framework with a Novel Feature Selection Algorithm for Intelligent Diagnosis in Smart Healthcare. IEEE Transactions on Machine Learning in Communications and Networking, 2, 370–383. https://doi.org/10.1109/tmlcn.2024.3374253.

[11] Taimoor, N., & Rehman, S. (2022). Reliable and Resilient AI and IoT-Based Personalised Healthcare Services: A Survey. IEEE Access, 10, 535–563. https://doi.org/10.1109/access.2021.3137364.

[12] Ahmed, S. F., Sharmin, S., Kuldeep, S. A., Lameesa, A., Alam, Md. S. B., Liu, G., & Gandomi, A. H. (2025). Transformative impacts of the internet of medical things on modern healthcare. Results in Engineering, 25, 103787. https://doi.org/10.1016/j.rineng.2024.103787.

[13] Ullah, A., Azeem, M., Ashraf, H., Alaboudi, A. A., Humayun, M., & Jhanjhi, N. (2021). Secure Healthcare Data Aggregation and Transmission in IoT—A Survey. IEEE Access, 9, 16849–16865. https://doi.org/10.1109/access.2021.3052850.

[14] Raina, R., & Jha, R. K. (2022). Intelligent and Interactive Healthcare System (I2HS) Using Machine Learning. IEEE Access, 10, 116402–116424. https://doi.org/10.1109/access.2022.3197878.

[15] Ahmed Alhaj, T., Abdulla, S. M., Iderss, M. A. E., Ali, A. A. A., Elhaj, F. A., Remli, M. A., & Gabralla, L. A. (2022). A Survey: To Govern, Protect, and Detect Security Principles on Internet of Medical Things (IoMT). IEEE Access, 10, 124777–124791. https://doi.org/10.1109/access.2022.3225038.

[16] Ashok, K., & Gopikrishnan, S. (2023). Statistical Analysis of Remote Health Monitoring Based IoT Security Models &amp; Deployments From a Pragmatic Perspective. IEEE Access, 11, 2621–2651. https://doi.org/10.1109/access.2023.3234632.

[17] Mazhar, T., Shah, S. F. A., Inam, S. A., Awotunde, J. B., Saeed, M. M., & Hamam, H. (2024). Analysis of integration of IoMT with blockchain: issues, challenges and solutions. Discover Internet of Things, 4(1). https://doi.org/10.1007/s43926-024-00078-1.

[18] Dautov, R., Distefano, S., & Buyya, R. (2019). Hierarchical data fusion for Smart Healthcare. Journal of Big Data, 6(1). https://doi.org/10.1186/s40537-019-0183-6

[19] Xames, Md. D., & Topcu, T. G. (2024). A Systematic Literature Review of Digital Twin Research for Healthcare Systems: Research Trends, Gaps, and Realization Challenges. IEEE Access, 12, 4099–4126. https://doi.org/10.1109/access.2023.3349379.

[20] Saraswat, D., Bhattacharya, P., Verma, A., Prasad, V. K., Tanwar, S., Sharma, G., Bokoro, P. N., & Sharma, R. (2022). Explainable AI for Healthcare 5.0: Opportunities and Challenges. IEEE Access, 10, 84486–84517. https://doi.org/10.1109/access.2022.3197671.

[21] Yang, F., Wu, Q., Hu, X., Ye, J., Yang, Y., Rao, H., Ma, R., & Hu, B. (2021). Internet-of-Things-Enabled Data Fusion Method for Sleep Healthcare Applications. IEEE Internet of Things Journal, 8(21), 15892–15905. https://doi.org/10.1109/jiot.2021.3067905

[22] Frasca, M., La Torre, D., Pravettoni, G., & Cutica, I. (2024). Explainable and interpretable artificial intelligence in medicine: a systematic bibliometric review. Discover Artificial Intelligence, 4(1). https://doi.org/10.1007/s44163-024-00114-7

[23] Javed, A. R., Saadia, A., Mughal, H., Gadekallu, T. R., Rizwan, M., Maddikunta, P. K. R., Mahmud, M., Liyanage, M., & Hussain, A. (2023). Artificial Intelligence for Cognitive Health Assessment: State-of-the-Art, Open Challenges and Future Directions. Cognitive Computation, 15(6), 1767–1812. https://doi.org/10.1007/s12559-023-10153-4

[24] Gupta, A., & Singh, A. (2022). Healthcare 4.0: recent advancements and futuristic research directions. Wireless Personal Communications, 129(2), 933–952. https://doi.org/10.1007/s11277-022-10164-8

[25] Mahmmod, B. M., Naser, M. A., Al-Sudani, A. H. S., Alsabah, M., Mohammed, H. J., Alaskar, H., Almarshad, F., Hussain, A., & Abdulhussain, S. H. (2024). Patient Monitoring System Based on Internet of Things: A Review and Related Challenges With Open Research Issues. IEEE Access, 12, 132444–132479. https://doi.org/10.1109/access.2024.3455900

[26] He, P., Huang, D., Wu, D., He, H., Wei, Y., Cui, Y., Wang, R., & Peng, L. (2024). A survey of internet of medical things: technology, application and future directions. Digital Communications and Networks. https://doi.org/10.1016/j.dcan.2024.11.013

[27] Hireche, R., Mansouri, H., & Pathan, A.-S. K. (2022). Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis. Journal of Cybersecurity and Privacy, 2(3), 640-661. https://doi.org/10.3390/jcp2030033

[28] Routray, S., Ghosh, U., Li, X., & Rabie, K. (2024). Editorial AI Driven Internet of Medical Things for Smart Healthcare Applications: Challenges and Future Trends. IEEE Journal of Biomedical and Health Informatics, 28(6), 3279–3281. https://doi.org/10.1109/jbhi.2024.3399289

[29] Wazid, M., Singh, J., Das, A. K., Shetty, S., Khan, M. K., & Rodrigues, J. J. P. C. (2022). ASCP-IoMT: AI-Enabled Lightweight Secure Communication Protocol for Internet of Medical Things. IEEE Access, 10, 57990–58004. https://doi.org/10.1109/access.2022.3179418

[30] El-deep, S. E., Abohany, A. A., Sallam, K. M., & El-Mageed, A. A. A. (2025). A comprehensive survey on impact of applying various technologies on the internet of medical things. Artificial Intelligence Review, 58(3). https://doi.org/10.1007/s10462-024-11063-z

[31] Batko, K., & Ślęzak, A. (2022). The use of Big Data Analytics in healthcare. Journal of Big Data, 9(1). https://doi.org/10.1186/s40537-021-00553-4

[32] Habuza, T., Navaz, A. N., Hashim, F., Alnajjar, F., Zaki, N., Serhani, M. A., & Statsenko, Y. (2021). AI applications in robotics, diagnostic image analysis and precision medicine: Current limitations, future trends, guidelines on CAD systems for medicine. Informatics in Medicine Unlocked, 24, 100596. https://doi.org/10.1016/j.imu.2021.100596

[33] Adavoudi Jolfaei, A., Aghili, S. F., & Singelee, D. (2021). A Survey on Blockchain-Based IoMT Systems: Towards Scalability. IEEE Access, 9, 148948–148975. https://doi.org/10.1109/access.2021.3117662

[34] Pustokhina, I. V., Pustokhin, D. A., Gupta, D., Khanna, A., Shankar, K., & Nguyen, G. N. (2020). An Effective Training Scheme for Deep Neural Network in Edge Computing Enabled Internet of Medical Things (IoMT) Systems. IEEE Access, 8, 107112–107123. https://doi.org/10.1109/access.2020.3000322

[35] Awotunde, J. B., Sur, S. N., Jimoh, R. G., Aremu, D. R., Do, D.-T., & Lee, B. M. (2023). FL_GIoT: Federated Learning Enabled Edge-Based Green Internet of Things System: A Comprehensive Survey. IEEE Access, 11, 136150–136165. https://doi.org/10.1109/access.2023.3335245

[36] Verma, P., Tiwari, R., Hong, W.-C., Upadhyay, S., & Yeh, Y.-H. (2022). FETCH: A Deep Learning-Based Fog Computing and IoT Integrated Environment for Healthcare Monitoring and Diagnosis. IEEE Access, 10, 12548–12563. https://doi.org/10.1109/access.2022.3143793

[37] Sindhuja, R., Kapse, A. S., & Kapse, A. S. (2023). A survey of Internet of Medical Things (IoMT) applications, architectures, and challenges in smart healthcare systems. *ITM Web Conferences*, *56*, 05013. https://doi.org/10.1051/itmconf/20235605013

[38] Awad, A. I., Fouda, M. M., Khashaba, M. M., Mohamed, E. R., & Hosny, K. M. (2023). Utilization of mobile edge computing on the Internet of Medical Things: A survey. ICT Express, 9(3), 473–485. https://doi.org/10.1016/j.icte.2022.05.006

[39] Iranpak, S., Shahbahrami, A., & Shakeri, H. (2021). Remote patient monitoring and classifying using the internet of things platform combined with cloud computing. Journal of Big Data, 8(1). https://doi.org/10.1186/s40537-021-00507-w

[40] Paganelli, A. I., Velmovitsky, P. E., Miranda, P., Branco, A., Alencar, P., Cowan, D., Endler, M., & Morita, P. P. (2022). A conceptual IoT-based early-warning architecture for remote monitoring of COVID-19 patients in wards and at home. Internet of Things, 18, 100399. https://doi.org/10.1016/j.iot.2021.100399

[41] Mohammed, K. I., Zaidan, A. A., Zaidan, B. B., Albahri, O. S., Alsalem, M. A., Albahri, A. S., Hadi, A., & Hashim, M. (2019). Real-Time Remote-Health Monitoring Systems: a Review on Patients Prioritisation for Multiple-Chronic Diseases, Taxonomy Analysis, Concerns and Solution Procedure. Journal of Medical Systems, 43(7). https://doi.org/10.1007/s10916-019-1362-x

[42] Allam, A. H., Gomaa, I., Zayed, H. H., & Taha, M. (2024). IoT-based eHealth using blockchain technology: a survey. Cluster Computing, 27(6), 7083–7110. https://doi.org/10.1007/s10586-024-04357-y

[43] Wagan, S. A., Koo, J., Siddiqui, I. F., Attique, M., Shin, D. R., & Qureshi, N. M. F. (2022). Internet of medical things and trending converged technologies: A comprehensive review on real-time applications. Journal of King Saud University - Computer and Information Sciences, 34(10), 9228–9251. https://doi.org/10.1016/j.jksuci.2022.09.005

[44] LaBoone, P. A., & Marques, O. (2024). Overview of the future impact of wearables and artificial intelligence in healthcare workflows and technology. International Journal of Information Management Data Insights, 4(2), 100294. https://doi.org/10.1016/j.jjimei.2024.100294

[45] Shaik, T., Tao, X., Li, L., Xie, H., & Velásquez, J. D. (2024). A survey of multimodal information fusion for smart healthcare: Mapping the journey from data to wisdom. Information Fusion, 102, 102040. https://doi.org/10.1016/j.inffus.2023.102040

[46] Ahmed, S., Esha, J. F., Rahman, Md. S., Kaiser, M. S., Hosen, A. S. M. S., Ghimire, D., & Park, M. J. (2024). Exploring Deep Learning and Machine Learning Approaches for Brain Hemorrhage Detection. IEEE Access, 12, 45060–45093. https://doi.org/10.1109/access.2024.3376438

[47] Mamun, A. A., Azam, S., & Gritti, C. (2022). Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction. IEEE Access, 10, 5768–5789. https://doi.org/10.1109/access.2022.3141079

[48] Masciari, E., Umair, A., & Ullah, M. H. (2024). A Systematic Literature Review on AI-Based Recommendation Systems and Their Ethical Considerations. IEEE Access, 12, 121223–121241. https://doi.org/10.1109/access.2024.3451054

[49] Darbandi, M., Alrasheedi, A. F., Alnowibet, K. A., Javaheri, D., & Mehbodniya, A. (2022). Integration of cloud computing with the Internet of things for the treatment and management of the COVID-19 pandemic. Information Systems and E-Business Management. https://doi.org/10.1007/s10257-022-00580-5

[50] Yaacoub, J.-P. A., Noura, M., Noura, H. N., Salman, O., Yaacoub, E., Couturier, R., & Chehab, A. (2020). Securing internet of medical things systems: Limitations, issues and recommendations. Future Generation Computer Systems, 105, 581–606. https://doi.org/10.1016/j.future.2019.12.028

[51] Arellanes, D., & Lau, K.-K. (2020). Evaluating IoT service composition mechanisms for the scalability of IoT systems. Future Generation Computer Systems, 108, 827–848. https://doi.org/10.1016/j.future.2020.02.073

[52] Mohammadi, V., Rahmani, A. M., Darwesh, A. M., & Sahafi, A. (2019). Trust-based recommendation systems in Internet of Things: a systematic literature review. Human-Centric Computing and Information Sciences, 9(1). https://doi.org/10.1186/s13673-019-0183-8

[53] Alzoubi, Y. I., Gill, A., & Mishra, A. (2022). A systematic review of the purposes of Blockchain and fog computing integration: classification and open issues. Journal of Cloud Computing, 11(1). https://doi.org/10.1186/s13677-022-00353-y

[54] Bathula, A., Gupta, S. K., Merugu, S., Saba, L., Khanna, N. N., Laird, J. R., Sanagala, S. S., Singh, R., Garg, D., Fouda, M. M., & Suri, J. S. (2024). Blockchain, artificial intelligence, and healthcare: the tripod of future—a narrative review. Artificial Intelligence Review, 57(9). https://doi.org/10.1007/s10462-024-10873-5

[55] Zeydan, E., Arslan, S. S., & Liyanage, M. (2024). Managing Distributed Machine Learning Lifecycle for Healthcare Data in the Cloud. IEEE Access, 12, 115750–115774. https://doi.org/10.1109/access.2024.3443520

[56] Doménech, J., Martin-Faus, I. V., Mhiri, S., & Pegueroles, J. (2024). Ensuring patient safety in IoMT: A systematic literature review of behavior-based intrusion detection systems. Internet of Things, 28, 101420. https://doi.org/10.1016/j.iot.2024.101420

[57] Hernandez-Jaimes, M. L., Martinez-Cruz, A., Ramírez-Gutiérrez, K. A., & Feregrino-Uribe, C. (2023). Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures. Internet of Things, 23, 100887. https://doi.org/10.1016/j.iot.2023.100887

[58] Humayun, M., Tariq, N., Alfayad, M., Zakwan, M., Alwakid, G., & Assiri, M. (2024). Securing the Internet of Things in Artificial Intelligence Era: A Comprehensive Survey. IEEE Access, 12, 25469–25490. https://doi.org/10.1109/access.2024.3365634

[59] Khatun, M. A., Memon, S. F., Eising, C., & Dhirani, L. L. (2023). Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation. IEEE Access, 11, 145869–145896. https://doi.org/10.1109/access.2023.3346320

[60] Jagatheesaperumal, S. K., Pham, Q.-V., Ruby, R., Yang, Z., Xu, C., & Zhang, Z. (2022). Explainable AI Over the Internet of Things (IoT): Overview, State-of-the-Art and Future Directions. IEEE Open Journal of the Communications Society, 3, 2106–2136. https://doi.org/10.1109/ojcoms.2022.3215676

[61] Sadeghi, Z., Alizadehsani, R., CIFCI, M. A., Kausar, S., Rehman, R., Mahanta, P., Bora, P. K., Almasri, A., Alkhawaldeh, R. S., Hussain, S., Alatas, B., Shoeibi, A., Moosaei, H., Hladík, M., Nahavandi, S., & Pardalos, P. M. (2024). A review of explainable artificial intelligence in healthcare. Computers and Electrical Engineering, 118(Part A), 109370. https://doi.org/10.1016/j.compeleceng.2024.109370

[62] Bharati, S., Mondal, M. R. H., & Podder, P. (2024). A Review on Explainable Artificial Intelligence for Healthcare: Why, How, and When? IEEE Transactions on Artificial Intelligence, 5(4), 1429–1442. https://doi.org/10.1109/tai.2023.3266418

[63] Wang, S., Qureshi, M. A., Miralles-Pechuán, L., Huynh-The, T., Gadekallu, T. R., & Liyanage, M. (2024). Explainable AI for 6G Use Cases: Technical Aspects and Research Challenges. IEEE Open Journal of the Communications Society, 5, 2490–2540. https://doi.org/10.1109/ojcoms.2024.3386872

[64] Artificial Intelligence and Machine Learning in Health Care and Medical Sciences. (2024). In G. J. Simon & C. Aliferis (Eds.), Health Informatics. Springer International Publishing. https://doi.org/10.1007/978-3-031-39355-6

[65] Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). 5G technology for healthcare: Features, serviceable pillars, and applications. Intelligent Pharmacy, 1(1), 2–10. https://doi.org/10.1016/j.ipha.2023.04.001

[66] Javaid, M., Haleem, A., & Singh, R. P. (2024). Health informatics to enhance the healthcare industry's culture: An extensive analysis of its features, contributions, applications and limitations. Informatics and Health, 1(2), 123–148. https://doi.org/10.1016/j.infoh.2024.05.001

[67] Desingh, V., & R, B. (2021). Internet of Things adoption barriers in the Indian healthcare supply chain: An ISM-fuzzy MICMAC approach. The International Journal of Health Planning and Management, 37(1), 318–351. Portico. https://doi.org/10.1002/hpm.3331

[68] Putra, K. T., Arrayyan, A. Z., Hayati, N., Firdaus, Damarjati, C., Bakar, A., & Chen, H.-C. (2024). A Review on the Application of Internet of Medical Things in Wearable Personal Health

Monitoring: A Cloud-Edge Artificial Intelligence Approach. IEEE Access, 12, 21437–21452. https://doi.org/10.1109/access.2024.3358827

[69] Laghari, A. A., Li, H., Karim, S., Hyder, W., Shoulin, Y., Khan, A. A., & Laghari, R. A. (2024). Internet of multimedia things (IoMT): A review. The Review of Socionetwork Strategies. https://doi.org/10.1007/s12626-024-00175-1

[70] Cardoso, L. F. de S., Kimura, B. Y. L., & Zorzal, E. R. (2023). Towards augmented and mixed reality on future mobile networks. Multimedia Tools and Applications, 83(3), 9067–9102. https://doi.org/10.1007/s11042-023-15301-4

[71] Gautam, A., Mahajan, R., & Zafar, S. (2020). QoS Optimization in Internet of Medical Things for Sustainable Management. Cognitive Internet of Medical Things for Smart Healthcare, 163–179. https://doi.org/10.1007/978-3-030-55833-8_10

[72] Ghadi, Y. Y., Shah, S. F. A., Mazhar, T., Shahzad, T., Ouahada, K., & Hamam, H. (2024). Enhancing patient healthcare with mobile edge computing and 5G: challenges and solutions for secure online health tools. Journal of Cloud Computing, 13(1). https://doi.org/10.1186/s13677-024-00654-4

[73] Albahri, A. S., Zaidan, A. A., Albahri, O. S., Zaidan, B. B., Hashim, M., & Alamoodi, A. H. (2021). Systematic review of artificial intelligence techniques in the Internet of Medical Things: Applications, challenges and solutions. *Sustainable Cities and Society, 72,* 103069. https://doi.org/10.1016/j.scs.2021.103069

[74] Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K.-S. (2015). The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access, 3,* 678–708. https://doi.org/10.1109/access.2015.2437951

[75] Rejeb, A., Rejeb, K., Treiblmaier, H., Appolloni, A., Alghamdi, S., Alhasawi, Y., & Iranmanesh, M. (2023). The Internet of Things (IoT) in healthcare: Taking stock and moving forward. Internet of Things, 22, 100721. https://doi.org/10.1016/j.iot.2023.100721

[76] Yıldırım, E., Cicioğlu, M., & Çalhan, A. (2023). Fog-cloud architecture-driven Internet of Medical Things framework for healthcare monitoring. Medical &amp; Biological Engineering &amp; Computing, 61(5), 1133–1147. https://doi.org/10.1007/s11517-023-02776-4

[77] Punia, A., Gulia, P., Gill, N. S., Ibeke, E., Iwendi, C., & Shukla, P. K. (2024). A systematic review on blockchain-based access control systems in cloud environment. Journal of Cloud Computing, 13(1). https://doi.org/10.1186/s13677-024-00697-7

[78] Vyas, A., Lin, P.-C., Hwang, R.-H., & Tripathi, M. (2024). Privacy-Preserving Federated Learning for Intrusion Detection in IoT Environments: A Survey. IEEE Access, 12, 127018–127050. https://doi.org/10.1109/access.2024.3454211

[79] Liu, K., Yan, Z., Liang, X., Kantola, R., & Hu, C. (2024). A survey on blockchain-enabled federated learning and its prospects with digital twin. Digital Communications and Networks, 10(2), 248–264. https://doi.org/10.1016/j.dcan.2022.08.001

[80] Alamri, B., Crowley, K., & Richardson, I. (2022). Blockchain-Based Identity Management Systems in Health IoT: A Systematic Review. IEEE Access, 10, 59612–59629. https://doi.org/10.1109/access.2022.3180367

[81] Nauman, A., Qadri, Y. A., Amjad, M., Zikria, Y. B., Afzal, M. K., & Kim, S. W. (2020). Multimedia Internet of Things: A Comprehensive Survey. IEEE Access, 8, 8202–8250. https://doi.org/10.1109/access.2020.2964280

[82] Aledhari, M., Razzak, R., Qolomany, B., Al-Fuqaha, A., & Saeed, F. (2022). Biomedical IoT: Enabling Technologies, Architectural Elements, Challenges, and Future Directions. IEEE Access, 10, 31306–31339. https://doi.org/10.1109/access.2022.3159235

[83] Erdiwansyah, Mahidin, Husin, H., Nasaruddin, Zaki, M., & Muhibbuddin. (2021). A critical review of the integration of renewable energy sources with various technologies. Protection and Control of Modern Power Systems, 6(1). https://doi.org/10.1186/s41601-021-00181-3

[84] Thottempudi, P., Konduru, R. M., Valiveti, H. B., Kuraparthi, S., & Kumar, V. (2025). Digital health resilience: IoT solutions in pandemic response and future healthcare scenarios. Discover Sustainability, 6(1). https://doi.org/10.1007/s43621-025-00886-7

[85] Mwanza, J., Telukdarie, A., & Igusa, T. (2023). Impact of industry 4.0 on healthcare systems of low- and middle- income countries: a systematic review. Health and Technology, 13(1), 35–52. https://doi.org/10.1007/s12553-022-00714-2

[86] Moghadam, M. P., Moghadam, Z. A., Qazani, M. R. C., Pławiak, P., & Alizadehsani, R. (2024). Impact of Artificial Intelligence in Nursing for Geriatric Clinical Care for Chronic Diseases: A Systematic Literature Review. IEEE Access, 12, 122557–122587. https://doi.org/10.1109/access.2024.3450970

[87] Liwen, Z., Qamar, F., Liaqat, M., Nour Hindia, M., & Akram Zainol Ariffin, K. (2024). Toward Efficient 6G IoT Networks: A Perspective on Resource Optimization Strategies, Challenges, and Future Directions. IEEE Access, 12, 76606–76633. https://doi.org/10.1109/access.2024.3405487

[88] Arpitha, T., Chouhan, D., & Shreyas, J. (2024). A Hybrid Optimization Approach to Enhance Source Location Privacy for IoT Healthcare. IEEE Access, 12, 132801–132816. https://doi.org/10.1109/access.2024.3452750