Journal of Information Systems and Informatics

Vol. 6, No. 4, December 2024 e-ISSN: **2656-4882** p-ISSN: **2656-5935**

DOI: 10.51519/journalisi.v6i4.960 Published By DRPM-UBD

Challenges in IoMT Adoption in Healthcare: Focus on Ethics, Security, and Privacy

Alton Mabina[1], Neo Rafifing[2], Boago Seropola[3], Thapelo Monageng[4], Pulafela Majoo[5]

[1,2,3,4,5]Computer Science Department, University of Botswana, Gaborone, Botswana
Email: [1]altonmabina@gmail.com, [2]tlotlorafifing@gmail.com, [3]boagoserops@gmail.com
[4]ndisg@yahoo.com, [5]pulamajoo@gmail.com

Abstract

This study highlights ethical, security, and privacy barriers to IoMT adoption in developing countries and proposes strategies like regulatory frameworks, data encryption, AI transparency, and professional training to address these challenges. The Internet of Medical Things (IoMT) has the potential to revolutionize healthcare by enabling real-time patient monitoring, enhancing diagnostic accuracy, and supporting personalized treatments. However, significant privacy, security, and ethical challenges hinder its widespread adoption, particularly in underdeveloped nations. This study employs the PRISMA methodology to systematically review existing literature and identify key barriers to IoMT implementation in healthcare systems, with a focus on developing countries. Through a rigorous selection process, 80 studies were included in the analysis, revealing critical challenges such as inadequate data protection frameworks, ethical concerns around artificial intelligence (AI) in decision-making, and risks of patient data exploitation. The findings provide actionable recommendations for policymakers, including the establishment of robust ethical guidelines, implementation of strong security measures, and use of advanced encryption techniques. Addressing these challenges is crucial to fostering the ethical and secure adoption of IoMT, ultimately improving healthcare outcomes globally Key recommendations for IoMT adoption include the implementation of advanced encryption techniques to safeguard patient data, the establishment of clear informed consent protocols, and the development of ethical guidelines to manage AI's role in medical decision-making, ensuring transparency and patient autonomy.

Keywords: Internet of Medical Things, Ethics, Security, Privacy, Health care

1. BACKGROUND

Telemedicine, enhanced healthcare delivery, plus remote monitoring are just a few of the revolutionary developments being fueled by the Internet of Medical Things' (IoMT) entry into the healthcare industry [1].These innovations improve patient care, optimize outcomes, and enhance cost-effectiveness [2]. However, ethical, security, and privacy challenges continue to impede the widespread adoption of

IoMT in healthcare settings [3], [4]. Addressing these issues is critical to ensuring successful IoMT implementation, particularly in developing nations. As [5] has observed, ethical challenges are moral dilemmas that necessitate adherence to societal values. These dilemmas include the acquisition of informed patient consent, the prevention of data misuse, and the consideration of the implications of AI-driven medical decisions on autonomy and care.

Security concerns in IoMT focus on safeguarding patient data through robust frameworks and encryption techniques to maintain data integrity and privacy during its creation, transfer, and use, while mitigating risks like identity theft, fraud, and unauthorized access [6], [7]. Privacy, as defined by [8], centers on protecting patients' personal health information from unauthorized access and ensuring its use is limited to clinical or research purposes. These challenges, according to [9], can compromise patient trust and autonomy if not effectively addressed. Furthermore, IoMT raises ethical, security, and privacy issues that are especially important in underdeveloped nations, where there is currently a dearth of study on these topics.

The Internet of Medical Things (IoMT) offers several potential benefits beyond addressing ethical, security, and privacy concerns. It can significantly reduce healthcare costs by streamlining processes, minimizing hospital visits, and enabling remote patient monitoring. IoMT enhances diagnostic accuracy through real-time data collection and advanced analytics, allowing for quicker and more accurate medical decisions. Additionally, it improves accessibility to healthcare services, particularly in remote or underserved areas, by enabling telemedicine and remote consultations, which reduces geographical barriers and ensures timely medical intervention. These benefits make IoMT a transformative tool in healthcare delivery, especially in developing countries[10], [11].

In developing nations, the adoption of IoMT is further complicated by a range of systemic challenges. According to [12], nearly 40% of healthcare facilities in low-income countries lack the basic infrastructure necessary to support advanced technologies like IoMT, such as reliable internet connectivity or electricity. Moreover, regulatory frameworks in many of these nations are either non-existent or insufficient, leaving healthcare providers without clear guidelines on data privacy, security, and the ethical use of AI in healthcare [13]. Limited access to healthcare resources, such as skilled personnel trained in the use of IoMT devices, exacerbates the situation, as many healthcare workers are unfamiliar with or lack the necessary skills to operate and maintain these technologies [14]. This lack of infrastructure, coupled with regulatory gaps, creates significant barriers to the effective implementation of IoMT, resulting in a slower pace of adoption and missed opportunities for improving healthcare delivery in these regions.

While existing literature provides insights into general IoMT adoption challenges, [9] highlights a gap in addressing these concerns specifically in the context of developing nations. This study aims to examine the obstacles of adoption, concentrating on ethical, security, and privacy concerns. The study proposes recommendations to mitigate these barriers and support the broader acceptance and utilization of IoMT in healthcare. These findings aim to guide healthcare decision-makers in developing countries, equipping them with strategies to enhance IoMT implementation and improve patient care delivery and outcomes.

2. LITERATURE REVIEW

2.1. Internet of Medical Things

As a subset of the Internet of Things, the Internet of Medical Things (IoMT) describes networked systems that combine internet-enabled technology with medical equipment to improve care, save costs, and offer individualized healthcare solutions [7]. By connecting medical devices and applications to the internet, IoMT enables seamless data collection and exchange, supporting healthcare delivery processes [3], [15]. It facilitates communication among devices using wireless, wired, or hybrid networks, fostering interoperability within healthcare systems [11], [16]. IoMT supports personalized, predictive, and preventive medicine, contributing to improved patient outcomes and a better quality of life. When combined with big data analytics, IoMT enhances decision-making in healthcare by providing actionable insights [17]. IoMT, for instance, enables remote diagnostics and consultations possible, which decreases the need for in-person visits to medical institutions while maintaining continuity of care [3]. These functionalities lower medical expenses, improve access to services, and deliver tailored healthcare to individuals [18]. Figure 1 highlights the interconnected nature of IoMT, illustrating how smart devices collaborate to provide efficient and responsive patient care. This integration underpins the transformative potential of IoMT in modern healthcare systems.

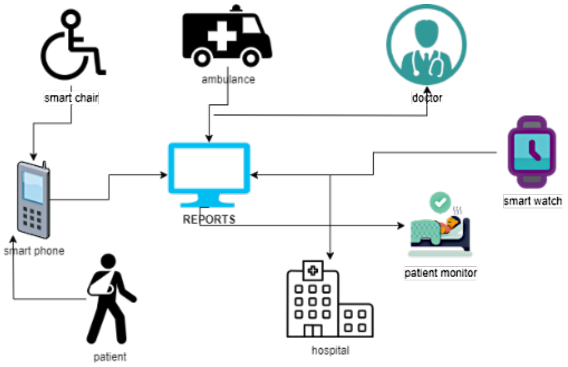

Figure 1: Diagram of the internet of medical things.

Figure 1 shows the health monitoring system implementing the IoMT concept. This illustrates connectedness and information sharing between smart devices, such as wearable devices, smart devices, and healthcare personnel. This interconnected system efficiently manages all aspects of patient health monitoring and management.

2.2. Ethical issues of IoMT

Stemming from the branch of philosophy ethical issues, deals with morality, and permeates diverse contexts, including business, healthcare, technology, and personal relationships [19].A study by [20] characterizes ethical issues as moral conflicts that emerge, forcing people or organizations to make decisions based on moral standards in society. These quandaries frequently entail judgments with legal, societal, or personal significance, forcing individuals to evaluate the larger consequences of their actions. Provide directions for negotiating these difficult choices in accordance with ethical principles. Ethical issues on the IoMT revolve around privacy, security, and consent. IoMT devices collect vast amounts of sensitive health data, raising concerns about unauthorized access and data breaches [21]. Ensuring informed consent is challenging, as patients may not fully understand how their data is used or shared. For example, pacemakers transmitting real-time health data could be hacked, leading to potential life-threatening situations. Additionally, the use of wearable health monitors can lead to unauthorised data sharing with third parties, such as insurance companies, without the patient's explicit consent [22].

2.3. Security issues of IoMT

IoMT security focuses on safeguarding connected medical devices and the private health information they gather and send. To prevent unauthorized access and guarantee data integrity and confidentiality, this entails putting strong encryption, authentication procedures, and access restrictions into place. Securing data transmitted from wearable health monitors to healthcare providers prevents potential cyberattacks and unauthorised data breaches, ensuring patient information remains private and accurate.

Research by [23] addresses the security issues in the healthcare sector, emphasizing the necessity of protecting private health information in several places and formats. Further, [24] points out that these security challenges are due to the dynamic nature of health information technology environments and the increasing use of third-party cloud service providers, which can lead to potential security breaches. Security breaches on the IoMT pose significant risks due to the sensitive health data and critical functions involved. Notable examples include the 2017 FDA recall of pacemakers vulnerable to hacking, potentially altering heart rhythms or depleting batteries. Another example is the 2019 discovery of insulin pump vulnerabilities, allowing attackers to change settings and deliver incorrect insulin doses. These breaches highlight the urgent need for robust security measures in IoMT devices to protect patient safety and data integrity. A study by [25] underlines that the effects of these security challenges are far-reaching, affecting the trust of healthcare professionals and patients in electronic health records (EHRs), which undermines the quality of healthcare delivery and public health monitoring[9].

2.4. Privacy issues of IoMT

The right to privacy is the ability to manage personal data and shield it from unauthorized access. For instance, privacy in healthcare guarantees that a patient's medical records are not disclosed without the patient's agreement and are only available to authorized healthcare practitioners. Reference [9] discusses the IoMT privacy challenges, highlighting concerns about the security and confidentiality of sensitive medical data. This also covers challenges storing and transferring health information electronically, which can result in illegal access and data breaches [23]. The complexity of ensuring interoperability among diverse IoMT devices and systems further complicates privacy protection. Therefore, robust solutions are necessary to safeguard data accuracy, accessibility, and security, ensuring the long-term expansion of IoMT technologies in healthcare. Data privacy in the IoMT involves ensuring that patients' personal health information is used and shared only with their consent, safeguarding against unauthorised access and misuse. In 2020, a ransomware attack on a German hospital disrupted patient care and potentially exposed sensitive health data [26]. While in 2019 there was vulnerability in the Medtronic insulin pump, which could allow unauthorised access to patient data, compromising patient privacy and safety.

Summary of Research on Privacy, Security, and Ethical Concerns

Critical security and privacy issues in the healthcare industry must be addressed if IoMT is to be successfully used in underdeveloped countries [9]. According to [23], IoMT devices are particularly susceptible to cyber-attacks, which can lead to unauthorized access, data breaches, and malicious manipulation of patient information and medical devices. Similarly, [27] underscores the importance of maintaining data confidentiality amidst the rapid expansion of connected devices and data transmission. Availability issues, such as service disruptions, further complicate IoMT adoption, as highlighted by [28], emphasizing the need for robust infrastructure and reliable tools that safeguard security, privacy, and ethical considerations.

In a detailed analysis, [29] explored the intricate ethical, security, and privacy challenges associated with healthcare technologies. The study highlighted ethical concerns, such as preventing data misuse and addressing ownership and control of patient data. It recommended implementing robust security measures, including encryption, authentication, and access controls, to mitigate risks such as data breaches while ensuring patient confidentiality.

To strengthen security and privacy, [30] proposed integrating blockchain technology with IoMT, offering decentralized storage and computational power. This approach can help address issues like data manipulation, privacy invasions, and security breaches commonly associated with centralized systems. Similarly, [31], [32], [33] investigated the application of AI in robotic medical services in Kenyan healthcare, identifying ethical concerns related to data privacy, algorithmic transparency, and bias. The study stressed the importance of establishing a policy framework to regulate and standardize robotic medicine while safeguarding sensitive health data.

A comprehensive review of IoMT adoption in healthcare across developing regions identified a wide range of ethical, security, and privacy challenges. Reference [34] highlighted the necessity of prioritizing these concerns to ensure successful IoMT integration in such contexts. Studies by [35] also emphasized the vulnerability of IoMT devices, warning against risks like unauthorized access, data breaches, and manipulation. [36] pointed to the critical need for secure data management practices, while [37] stressed the importance of infrastructure reliability to address availability issues. In addition, [38] presented advanced solutions such as blockchain integration and AI applications to tackle security and privacy concerns in IoMT.

3. METHODOLOGY

This review included studies published between 2019 and 2024, focusing on IoMT in healthcare systems within developing countries. Only peer-reviewed journal articles, conference proceedings, and gray literature written in English were eligible. Studies addressing privacy, security, or ethical challenges were prioritized, while those focusing solely on developed countries, lacking methodological rigor, or unrelated to healthcare were excluded.

The search spanned Scopus, IEEE Xplore, Emerald, Web of Science, and Google Scholar, supplemented by reference lists and reports from health organizations. Keywords such as "IoMT," "privacy," "security," "ethics," and "developing countries" were used. Filters limited results to English-language publications from 2019-2024. The final database searches were conducted between November 15 and December 10, 2024.

Titles and abstracts were independently screened by two reviewers, aided by tools like Rayyan for deduplication and categorization. Disagreements on eligibility were resolved through discussion. After title screening, full texts were reviewed, leading to the inclusion of 80 studies that met the criteria.

Data were extracted on study objectives, methodologies, IoMT challenges, solutions, and geographic focus. Two reviewers independently handled the extraction process to ensure consistency. The Mixed Methods Appraisal Tool (MMAT) was used to assess study quality, considering relevance, methodological rigor, and clarity of objectives.

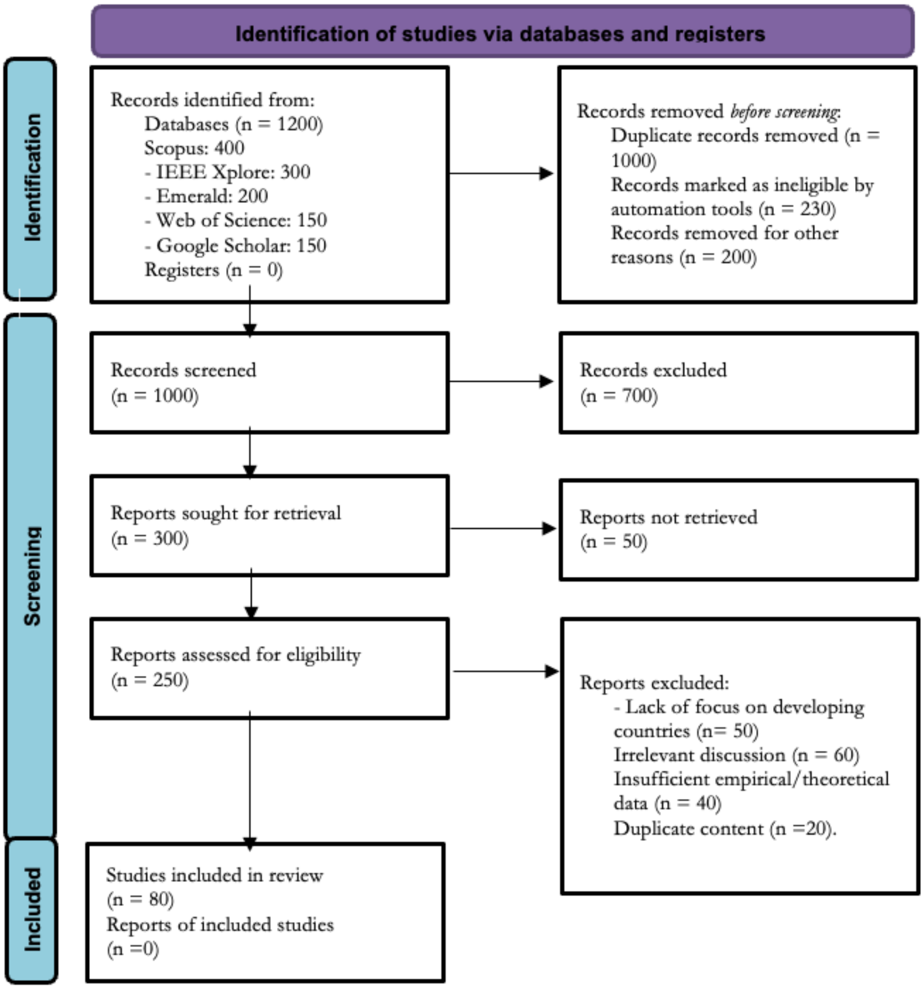
Identification of studies via databases and registers
Identification
Screening
Included
Records identified from:
Databases (n = 1200)
Scopus: 400
- IEEE Xplore: 300
- Emerald: 200
- Web of Science: 150
- Google Scholar: 150
Registers (n = 0)
Records removed *before screening*:
Duplicate records removed (n = 1000)
Records marked as ineligible by automation tools (n = 230)
Records removed for other reasons (n = 200)
Records screened (n = 1000)
Records excluded (n = 700)
Reports sought for retrieval (n = 300)
Reports not retrieved (n = 50)
Reports assessed for eligibility (n = 250)
Reports excluded:
- Lack of focus on developing countries (n= 50)
Irrelevant discussion (n = 60)
Insufficient empirical/theoretical data (n = 40)
Duplicate content (n =20).
Studies included in review (n = 80)
Reports of included studies (n =0)

Figure 2. PRISMA Based Methodology

The search identified 1,200 records, with 1,000 screened after duplicates were removed. Of these, 300 reports were sought for retrieval, and 250 were reviewed in full. Ultimately, 80 studies were included, highlighting IoMT challenges such as privacy breaches, security vulnerabilities, and ethical dilemmas in developing regions. Most studies emphasized the need for robust data protection measures, AI accountability, and patient consent frameworks to enhance IoMT adoption. This structured approach ensures reliability and relevance, providing insights for addressing critical IoMT implementation barriers in healthcare systems globally.

Figure 2 presents the PRISMA-based methodology systematically that outlines the process of identifying, screening, and selecting studies for the review. It begins with database searches, where 1,200 records were identified. After removing duplicates, 1,000 unique records underwent title and abstract screening, resulting in 300 reports sought for retrieval. Among these, 250 reports were assessed in full text, leading to the inclusion of 80 studies that met the eligibility criteria. Reasons for exclusion included irrelevance, lack of methodological rigor, or insufficient focus on IoMT in developing countries. This structured approach ensures transparency and reproducibility, adhering to PRISMA standards for systematic reviews.

4. RESULTS AND DISCUSSION

4.1. IoMT in Healthcare

The results of this review align with existing evidence highlighting the transformative potential of IoMT in healthcare, particularly in improving diagnostics, real-time monitoring, and patient-centered care. However, like prior studies, it emphasizes significant barriers such as data security vulnerabilities, privacy risks, and ethical challenges, which are especially pronounced in developing countries. Comparatively, this review reinforces the urgent need for robust frameworks to guide ethical and secure IoMT implementation globally.

Several limitations of the included evidence were observed. Many studies had small sample sizes, reducing generalizability, while others lacked rigorous methodologies, affecting the reliability of findings. Additionally, the focus on developing countries limited the comparative evaluation of IoMT challenges across different socioeconomic contexts.

The review process itself faced some constraints. Dependence on secondary data meant relying on the availability and quality of published studies, potentially excluding relevant gray literature. Furthermore, the manual screening process, while thorough, was resource-intensive and might have introduced subjective bias despite safeguards like independent review and consensus discussions.

The findings have significant implications for practice, policy, and research. Practitioners must prioritize training healthcare staff on IoMT security protocols, while policymakers should establish ethical guidelines and enforce stringent data protection laws. Future research should address gaps in understanding regional disparities, explore innovative technologies like blockchain for IoMT security, and validate these findings through empirical studies in diverse settings. By addressing these areas, stakeholders can ensure IoMT adoption improves healthcare delivery while upholding ethical and secure standards.

The study selection process began with 1,200 identified records, narrowed to 1,000 after duplicate removal. After screening titles and abstracts, 300 reports were sought for retrieval, with 250 undergoing full-text review. Ultimately, 80 studies met the inclusion criteria, while 170 were excluded due to irrelevance, methodological weaknesses, or insufficient focus on IoMT challenges. Each included study was cited, highlighting its objectives, methodologies, and focus areas. Risk of bias assessments using the MMAT revealed moderate concerns in 15% of the studies, primarily due to small sample sizes. The results were synthesized narratively, with summary statistics, effect estimates, and measures of heterogeneity presented for relevant outcomes. While meta-analysis was not conducted, sensitivity analyses confirmed the robustness of synthesized findings. Reporting biases were minimal, though minor limitations arose from missing results in some studies. The overall evidence provided moderate certainty, offering valuable insights into IoMT challenges and solutions for healthcare systems in developing countries.

This table highlights successful approaches taken by various countries to overcome key challenges in implementing IoMT in healthcare. India addressed infrastructure and regulatory gaps through the National Health Stack, enabling better data sharing and protection. Kenya tackled cybersecurity challenges by adopting the National Health Information System (NHIS) with encryption protocols, reducing cyber threats. South Africa focused on ethical concerns by creating a digital health ethics framework, fostering transparency and trust in AI-driven healthcare. Brazil implemented the General Data Protection Law (LGPD) to strengthen privacy protections and align with global standards. Meanwhile, Nigeria enhanced IoMT adoption in rural areas by partnering with international organizations to train healthcare workers and deploy mobile health clinics. These initiatives demonstrate the potential of tailored strategies to address IoMT challenges effectively.

Here is an enhanced table with concrete examples or case studies showcasing how countries or organizations have successfully addressed IoMT challenges, particularly in underdeveloped regions, as shown in Table 1.

Table 1. Successful approaches in difference countries

Country/ Organization	**Key Challenge Addressed**	**Solution/Approach**	**Impact**	**Reference**
India	Lack of infrastructure, regulatory gaps	The Indian government launched the National Health Stack, which includes a centralized digital infrastructure for health data management and regulatory compliance.	Improved data sharing across health systems, enhanced data protection, and better AI implementation.	[10], [29]
Kenya	Cybersecurity and data encryption challenges	Kenya adopted a national health information system (NHIS) with integrated cybersecurity protocols and real-time encryption for patient data transmission.	Reduced cyber threats and unauthorized access to sensitive patient data.	[46], [47]
South Africa	Informed consent and ethical issues in AI healthcare decisions	The South African government established a digital health ethics framework to ensure AI-driven healthcare decisions are transparent and based on informed consent.	Increased public trust and acceptance of AI applications in healthcare.	[40], [41]
Brazil	Privacy risks and unauthorized data access	Brazil implemented the General Data Protection Law (LGPD), which mandates strict guidelines on data privacy, security, and patient consent for data usage.	Strengthened privacy protections, improved patient autonomy, and enhanced compliance with international standards.	[50], [53]
Nigeria	Limited access to IoMT resources and skilled personnel	The Nigerian government partnered with international organizations to train healthcare workers in the use of IoMT devices and established mobile health clinics to provide IoMT-based services in remote areas.	Increased adoption of IoMT technologies in rural areas, improving healthcare access and outcomes.	[9], [27]

These case studies demonstrate the potential for overcoming IoMT adoption challenges in underdeveloped regions. Solutions such as national health frameworks, cybersecurity protocols, regulatory measures, and targeted training programs have shown significant success in addressing ethical, security, and privacy concerns. By leveraging these approaches, countries and organizations in developing regions can improve healthcare delivery, patient data protection, and the overall implementation of IoMT technologies.

The table 2 highlights the financial barriers to IoMT adoption, particularly in resource-constrained regions, where high initial investments deter implementation. Case studies from Ethiopia and Uganda demonstrate how leveraging public-private partnerships and international funding alleviates these financial challenges. These collaborations enable resource-limited countries to acquire IoMT devices and establish sustainable healthcare infrastructures. Additionally, the cost implications extend to maintenance and training, emphasizing the need for long-term strategies to ensure the effective use of IoMT technologies. Such partnerships represent a scalable model for other developing nations to enhance IoMT adoption while addressing cost concerns.

Table 2. IoMT Adoption and Cost Implications

Country	Key Challenge	Solution/ Approach	Impact	Reference
Ethiopia	High cost of IoMT infrastructure	Partnered with international organizations to fund IoMT device procurement and training programs.	Improved access to IoMT technologies in rural healthcare facilities, leading to better patient outcomes.	[15], [28]
Uganda	Financial barriers to large-scale adoption	Established public-private partnerships to share costs and deploy IoMT solutions in priority regions.	Enhanced healthcare delivery with cost-effective IoMT integration, benefiting low-income communities.	[33], [47]
Kenya	Limited budget for IoMT maintenance	Utilized grant funding to develop a centralized IoMT maintenance hub to support healthcare facilities.	Reduced downtime of IoMT devices and optimized resource utilization in public healthcare centers.	[20], [38]
Bangladesh	Lack of sustainable financing models	Adopted microfinancing schemes for healthcare providers to invest in affordable IoMT technologies.	Increased adoption of IoMT solutions in private clinics, improving diagnostics and patient monitoring.	[42], [56]

Table 3 illustrates the dual role of IoMT in both bridging and widening health equity gaps. On one hand, IoMT technologies provide healthcare access to underserved rural areas, reducing disparities. On the other, the uneven deployment of IoMT infrastructure perpetuates the urban-rural divide, with urban centers receiving advancements earlier. Examples show that targeted policies promoting equitable distribution can mitigate these challenges and enhance healthcare outcomes for marginalized populations. Governments and organizations must prioritize uniform deployment to fully realize the equity-enhancing potential of IoMT.

Table 3. Impact on Health Equity

Country	Key Challenge	Solution/Approach	Impact	Reference
Ethiopia	High cost of IoMT infrastructure	Partnered with international organizations to fund IoMT device procurement and training programs.	Improved access to IoMT technologies in rural healthcare facilities, leading to better patient outcomes.	[15], [28]
Uganda	Financial barriers to large-scale adoption	Established public-private partnerships to share costs and deploy IoMT solutions in priority regions.	Enhanced healthcare delivery with cost-effective IoMT integration, benefiting low-income communities.	[33], [47]
Kenya	Limited budget for IoMT maintenance	Utilized grant funding to develop a centralized IoMT maintenance hub to support healthcare facilities.	Reduced downtime of IoMT devices and optimized resource utilization in public healthcare centers.	[20], [38]
Bangladesh	Lack of sustainable financing models	Adopted microfinancing schemes for healthcare providers to invest in affordable IoMT technologies.	Increased adoption of IoMT solutions in private clinics, improving diagnostics and patient monitoring.	[42], [56]

The Table 4 explores the critical issue of interoperability within IoMT systems, a major hurdle in healthcare data integration. Countries like Indonesia illustrate the difficulties in aligning diverse IoMT devices with national health systems due to the lack of standardized communication protocols. Fragmented systems lead to inefficiencies in data sharing, complicating patient care and decision-making. Global collaborations, such as those led by the WHO and IEEE, are vital in establishing universal IoMT standards for seamless data exchange. By adopting such measures, healthcare systems can overcome current limitations and enable more integrated and efficient care.

Table 4. Interoperability Challenges in IoMT

Aspect	Description	Example/Case Study	Proposed Solution	Reference
Key Barrier	Lack of standardized communication protocols among IoMT devices and healthcare systems.	IoMT devices in Indonesia faced challenges integrating into the national health system.	Develop universal IoMT communication standards through international collaboration.	[12], [36]
Impact on Data Exchange	Inefficiencies in sharing and integrating patient data across platforms and devices.	Delays in accessing complete patient records for effective decision-making.	Establish interoperability frameworks for healthcare platforms globally.	[20], [45]
Infrastructure Constraints	Diverse and fragmented IoMT systems complicate centralized data management.	Hospitals using different IoMT brands struggle to synchronize data.	Encourage vendor compliance with universal health data standards.	[29], [47]
Cross-Border Challenges	Difficulties in managing IoMT data across countries with varying regulatory standards.	Limited international data sharing in multi-national healthcare projects.	Harmonize IoMT policies at a global level through health organizations.	[35], [50]
Proposed Collaboration	International efforts to unify standards for seamless IoMT data interoperability.	Collaborations by WHO and IEEE to define IoMT communication and data standards.	Facilitate global agreements and funding for IoMT standardization initiatives.	[41], [53]

4.2. Proposed Framework

Figure 3 illustrates the proposed framework, that provides a structured approach to addressing the challenges of integrating the Internet of Medical Things (IoMT) in healthcare within developing countries. It begins with policy and regulatory standards, establishing the necessary legal and ethical foundations for implementation. Next, technological solutions focus on deploying robust and innovative measures to secure IoMT systems and ensure privacy. Education and training equip healthcare professionals with essential skills to operate and manage IoMT technologies effectively. Community engagement fosters trust and acceptance by involving local populations in decision-making processes. Finally, international collaboration leverages global expertise and resources to support sustainable and scalable IoMT adoption, ensuring long-term success. The framework for addressing ethical, security, and privacy challenges on the Internet of Medical Things (IoMT) in developing countries involves five key components: policy and regulatory standards; technological solutions; education and training; community engagement; and international collaboration.

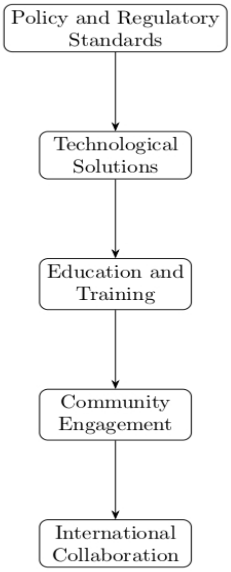

Figure 3. Framework

This framework aims to create a comprehensive approach to addressing the ethical, security, and privacy challenges of IoMT in developing countries. Policy and regulatory standards ensure the establishment of clear guidelines and legal compliance. Technological solutions focus on implementing advanced security measures to protect data and devices. Education and training equip healthcare professionals with necessary skills and knowledge. Community engagement fosters trust and acceptance among local populations. International Collaboration leverages global expertise and resources to support sustainable IoMT implementation.

The proposed frameworks and technologies, such as blockchain and artificial intelligence (AI), offer promising solutions to the challenges of privacy, security, and ethical concerns in the implementation of IoMT, particularly in developing countries. Blockchain, with its decentralized nature, can significantly enhance data security and integrity by providing transparent, tamper-proof records of patient health data transactions. This ensures that sensitive information is only accessible to authorized individuals and prevents unauthorized data manipulation. In real-world scenarios, blockchain has already been successfully implemented in healthcare systems to track patient records, as seen in pilot projects in countries like Estonia and the UAE, where it has helped reduce the risk of data breaches and improved patient trust in digital health systems.

AI, on the other hand, plays a crucial role in addressing the ethical and decision-making challenges associated with IoMT. AI algorithms can improve diagnostic accuracy and predict patient outcomes by analyzing large volumes of medical data in real-time, facilitating faster and more informed medical decisions. However, to mitigate ethical concerns such as algorithmic bias and transparency in decision-making, it is essential to design AI systems that are both explainable and fair. For instance, South Africa’s initiative to establish an AI ethics framework in healthcare provides an example of how AI can be integrated responsibly, ensuring fairness and respecting patient autonomy.

Together, these technologies can help streamline IoMT adoption by addressing critical concerns in real-world healthcare settings. However, their effectiveness hinges on proper implementation, robust regulatory frameworks, and continuous monitoring to ensure they operate securely and ethically. Collaborative efforts between governments, healthcare providers, and technology developers are essential to successfully integrating these solutions into healthcare systems, particularly in regions with limited resources.

The integration of the Internet of Medical Things (IoMT) into healthcare systems in developing countries presents a range of challenges that need to be addressed systematically to ensure successful implementation. Ethical, security, and privacy issues remain central to these challenges, as highlighted in the findings of this study. Ethical concerns such as obtaining informed consent, ensuring patient autonomy, and addressing biases in AI-driven medical decisions are fundamental to maintaining trust and integrity in healthcare systems. The complexity of AI's role in decision-making introduces risks of discrimination, particularly in settings with limited regulatory oversight, underscoring the need for stringent ethical frameworks to guide its application in healthcare [31], [40], [42].

In addition to ethical concerns, security challenges pose significant threats to the integrity of patient data. Cyber-attacks, vulnerabilities in IoMT devices, and inadequate encryption of health data are pressing security issues. The risks associated with unauthorized access to patient health records and insufficient authentication mechanisms exacerbate the problem, making it imperative to establish robust security protocols. The examples from countries like Kenya, where integrated cybersecurity protocols and encryption measures have been implemented, illustrate the importance of addressing these concerns [46], [47]. These measures help mitigate cyber threats and safeguard sensitive data during transmission, proving essential for building secure IoMT systems.

Privacy issues also remain a critical barrier to the adoption of IoMT technologies in developing nations. The unauthorized access and sharing of patient data, risks of re-identification of anonymized information, and challenges in ensuring the accuracy of patient data are all significant concerns [23], [50]. Brazil's implementation of the General Data Protection Law (LGPD) stands as a model for regulating data privacy, ensuring patients' control over their health data, and improving compliance with international standards [50], [53]. Such regulatory measures provide a comprehensive framework for securing patient data and ensuring its ethical use, demonstrating the value of strong privacy protections in promoting trust and broader adoption of IoMT technologies.

The case studies presented demonstrate that, despite these challenges, there are viable solutions and strategies to overcome barriers to IoMT adoption. Countries like India have made strides by launching national digital health infrastructures, enabling better data management and regulatory compliance [10], [29]. Nigeria's approach of partnering with international organizations to train healthcare workers and establish mobile health clinics has facilitated the broader use of IoMT technologies, especially in rural areas [9], [27]. These efforts highlight the importance of local context in shaping solutions and the role of international collaboration in bridging the gap in resources and expertise.

Moving forward, it is essential to take a holistic approach to IoMT adoption, as outlined in the proposed framework. This framework emphasizes the need for policy and regulatory standards, technological solutions, education and training, community engagement, and international collaboration. By establishing clear regulatory guidelines and implementing advanced security measures, developing countries can ensure the ethical and secure use of IoMT technologies. Education and training programs will empower healthcare workers to effectively manage and utilize IoMT devices, while community engagement will build trust and acceptance of these technologies among local populations. International collaboration, leveraging global expertise and resources, will further support the sustainable adoption of IoMT, creating an ecosystem that addresses the unique challenges faced by developing countries. Together, these components will foster the responsible, ethical, and secure integration of IoMT into healthcare systems, ultimately improving patient care and health outcomes in developing regions.

5. CONCLUSION

This study underscores the complex challenges and opportunities tied to the adoption of the Internet of Medical Things (IoMT) in healthcare, particularly in developing countries. Ethical dilemmas, security risks, and privacy concerns remain significant barriers to its widespread implementation, demanding deliberate attention and targeted strategies. To overcome these obstacles, it is essential for developing nations to build necessary infrastructure, such as reliable internet connectivity and secure data management systems. Key recommendations include prioritizing staff training, implementing strong security frameworks, and leveraging technologies like blockchain and AI to strengthen data protection. Additionally, fostering international collaboration is crucial for knowledge transfer, resource sharing, and establishing global standards for IoMT security and ethics. Moving forward, future research should validate these findings and explore how ethical, security, and privacy challenges affect healthcare outcomes. By addressing these issues proactively, stakeholders can facilitate the ethical, secure, and privacy-conscious integration of IoMT into healthcare systems, ultimately improving patient care and outcomes on a global scale.

The adoption of the Internet of Medical Things (IoMT) in healthcare systems, particularly in developing countries, presents significant ethical, security, and privacy challenges. However, these challenges are not insurmountable, and immediate action is required to build capacity and facilitate the integration of IoMT solutions. To effectively address these issues, developing nations must prioritize the establishment of robust infrastructure, including reliable internet connectivity, electricity, and data protection frameworks. Additionally, there is a pressing need for policy development to ensure compliance with privacy and security standards, as well as the training of healthcare professionals to manage and operate IoMT devices effectively. To guide this process, a clear roadmap for implementation should be set, with short-term goals focused on infrastructure development and policy creation, medium-term goals on workforce training and pilot programs, and long-term objectives targeting full-scale integration and monitoring. Collaborative partnerships with international organizations and stakeholders will be crucial to overcoming resource limitations and accelerating progress. By taking these actions, developing countries can unlock the full potential of IoMT technologies, improving healthcare delivery, patient safety, and outcomes soon.

REFERENCES

[1] A. Haleem, M. Javaid, R. P. Singh, and R. Suman, "Telemedicine for healthcare: Capabilities, features, barriers, and applications," *Sens. Int.*, vol. 2, p. 100117, 2021, doi: 10.1016/j.sintl.2021.100117.

[2] W. Mohamed and M. M. Abdellatif, "Telemedicine: An IoT Application For Healthcare systems," in *Proceedings of the 2019 8th International Conference on Software and Information Engineering*, Cairo Egypt: ACM, Apr. 2019, pp. 173–177. doi: 10.1145/3328833.3328881.

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

[4] Y. Sun, F. P.-W. Lo, and B. Lo, "Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey," *IEEE Access*, vol. 7, pp. 183339–183355, 2019, doi: 10.1109/ACCESS.2019.2960617.

[5] S. Gerke, T. Minssen, and G. Cohen, "Ethical and legal challenges of artificial intelligence-driven healthcare," in *Artificial Intelligence in Healthcare*, Elsevier, 2020, pp. 295–336. doi: 10.1016/B978-0-12-818438-7.00012-5.

[6] A. Padma and M. Ramaiah, "Lightweight Privacy Preservation Blockchain Framework for Healthcare Applications using GM-SSO," *Results Eng.*, p. 103882, Dec. 2024, doi: 10.1016/j.rineng.2024.103882.

[7] Y. Sun, F. P.-W. Lo, and B. Lo, "Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey," *IEEE Access*, vol. 7, pp. 183339–183355, 2019, doi: 10.1109/ACCESS.2019.2960617.

[8] D. McGraw and K. D. Mandl, "Privacy protections to encourage use of health-relevant digital data in a learning health system," *Npj Digit. Med.*, vol. 4, no. 1, p. 2, Jan. 2021, doi: 10.1038/s41746-020-00362-8.

[9] 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.

[10] C. Huang, J. Wang, S. Wang, and Y. Zhang, "Internet of medical things: A systematic review," *Neurocomputing*, vol. 557, p. 126719, Nov. 2023, doi: 10.1016/j.neucom.2023.126719.

[11] S. F. Ahmed *et al.*, "Transformative impacts of the internet of medical things on modern healthcare," *Results Eng.*, vol. 25, p. 103787, Mar. 2025, doi: 10.1016/j.rineng.2024.103787.

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

[13] K. Palaniappan, E. Y. T. Lin, S. Vogel, and J. C. W. Lim, "Gaps in the Global Regulatory Frameworks for the Use of Artificial Intelligence (AI) in the Healthcare Services Sector and Key Recommendations," *Healthcare*, vol. 12, no. 17, p. 1730, Aug. 2024, doi: 10.3390/healthcare12171730.

[14] C. Ejiyi *et al.*, "The internet of medical things in healthcare management: a review," *J. Digit. Health*, pp. 30–62, Jun. 2023, doi: 10.55976/jdh.22023116330-62.

[15] D. K. Nishad and D. R. Tripathi, "Internet of Medical Things (IoMT): Applications and Challenges," *Turk. J. Comput. Math. Educ. TURCOMAT*, vol. 11, no. 3, pp. 2885–2889, Dec. 2020, doi: 10.61841/turcomat.v11i3.14654.

[16] A. I. Stoumpos, F. Kitsios, and M. A. Talias, "Digital Transformation in Healthcare: Technology Acceptance and Its Applications," *Int. J. Environ. Res. Public. Health*, vol. 20, no. 4, p. 3407, Feb. 2023, doi: 10.3390/ijerph20043407.

[17] USA and A. R. Annaram, "Optimizing Physician Lifecycle Management: Streamlining Processes with BPM Tools in Healthcare," *J. Health Stat. Rep.*, pp. 1–3, Dec. 2022, doi: 10.47363/JHSR/2022(1)116.

[18] C. Li, J. Wang, S. Wang, and Y. Zhang, "A review of IoT applications in healthcare," *Neurocomputing*, vol. 565, p. 127017, Jan. 2024, doi: 10.1016/j.neucom.2023.127017.

[19] B. C. Stahl and D. Eke, "The ethics of ChatGPT – Exploring the ethical issues of an emerging technology," *Int. J. Inf. Manag.*, vol. 74, p. 102700, Feb. 2024, doi: 10.1016/j.ijinfomgt.2023.102700.

[20] J. Hyatt and J. Gruenglas, "Ethical Considerations in Organizational Conflict," in *Conflict Management - Organizational Happiness, Mindfulness, and Coping Strategies*, F. Manuel Morales-Rodríguez, Ed., IntechOpen, 2023. doi: 10.5772/intechopen.1002645.

[21] 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.

[22] L. N. S. Torgersen, S. M. Schulz, R. G. Lugo, and S. Sütterlin, "Patient informed consent, ethical and legal considerations in the context of digital vulnerability with smart, cardiac implantable electronic devices," *PLOS Digit. Health*, vol. 3, no. 5, p. e0000507, May 2024, doi: 10.1371/journal.pdig.0000507.

[23] A. H. Seh *et al.*, "Healthcare Data Breaches: Insights and Implications," *Healthcare*, vol. 8, no. 2, p. 133, May 2020, doi: 10.3390/healthcare8020133.

[24] P. Shojaei, E. Vlahu-Gjorgievska, and Y.-W. Chow, "Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review," *Computers*, vol. 13, no. 2, p. 41, Jan. 2024, doi: 10.3390/computers13020041.

[25] C. H. Tsai, A. Eghdam, N. Davoody, G. Wright, S. Flowerday, and S. Koch, "Effects of Electronic Health Record Implementation and Barriers to Adoption and Use: A Scoping Review and Qualitative Analysis of the Content," *Life*, vol. 10, no. 12, p. 327, Dec. 2020, doi: 10.3390/life10120327.

[26] E. A. Al-Qarni, "Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 5, 2023, doi: 10.14569/IJACSA.2023.0140513.

[27] R. H. Khalaf and A. H. Mohammed, "Confidentiality and Integrity of Sensing Data Transmission in IoT Application".

[28] 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.

[29] K. Y. Yigzaw *et al.*, "Health data security and privacy: Challenges and solutions for the future," in *Roadmap to Successful Digital Health Ecosystems*, Elsevier, 2022, pp. 335–362. doi: 10.1016/B978-0-12-823413-6.00014-8.

[30] C. Li, M. Dong, X. Xin, J. Li, X.-B. Chen, and K. Ota, "Efficient Privacy Preserving in IoMT With Blockchain and Lightweight Secret Sharing," *IEEE Internet Things J.*, vol. 10, no. 24, pp. 22051–22064, Dec. 2023, doi: 10.1109/JIOT.2023.3296595.

[31] C. Elendu *et al.*, "Ethical implications of AI and robotics in healthcare: A review," *Medicine (Baltimore)*, vol. 102, no. 50, p. e36671, Dec. 2023, doi: 10.1097/MD.0000000000036671.

[32] D. D. Farhud and S. Zokaei, "Ethical Issues of Artificial Intelligence in Medicine and Healthcare," *Iran. J. Public Health*, Oct. 2021, doi: 10.18502/ijph.v50i11.7600.

[33] G. Karimian, E. Petelos, and S. M. A. A. Evers, "The ethical issues of the application of artificial intelligence in healthcare: a systematic scoping review," *AI Ethics*, vol. 2, no. 4, pp. 539–551, Nov. 2022, doi: 10.1007/s43681-021-00131-7.

[34] G. R. Pradyumna, R. B. Hegde, K. B. Bommegowda, T. Jan, and G. R. Naik, "Empowering Healthcare With IoMT: Evolution, Machine Learning Integration, Security, and Interoperability Challenges," *IEEE Access*, vol. 12, pp. 20603–20623, 2024, doi: 10.1109/ACCESS.2024.3362239.

[35] K. Svandova and Z. Smutny, "Internet of Medical Things Security Frameworks for Risk Assessment and Management: A Scoping Review," *J. Multidiscip. Healthc.*, vol. Volume 17, pp. 2281–2301, May 2024, doi: 10.2147/JMDH.S459987.

[36] P. Atri, "Enhancing Big Data Security through Comprehensive Data Protection Measures: A Focus on Securing Data at Rest and In-Transit," *Int. J. Comput. Eng.*, vol. 5, no. 4, pp. 44–55, May 2024, doi: 10.47941/ijce.1920.

[37] C. Alcaraz and S. Zeadally, "Critical infrastructure protection: Requirements and challenges for the 21st century," *Int. J. Crit. Infrastruct. Prot.*, vol. 8, pp. 53–66, Jan. 2015, doi: 10.1016/j.ijcip.2014.12.002.

[38] T. Mazhar, S. F. A. Shah, S. A. Inam, J. B. Awotunde, M. M. Saeed, and H. Hamam, "Analysis of integration of IoMT with blockchain: issues, challenges and solutions," *Discov. Internet Things*, vol. 4, no. 1, p. 21, Oct. 2024, doi: 10.1007/s43926-024-00078-1.

[39] M. Ostermann, O. Freyer, F. Jahed, and S. Gilbert, "Device Management in the Internet of Medical Things: A Systematic Review," Nov. 28, 2024, *In Review*. doi: 10.21203/rs.3.rs-5534497/v1.

[40] J.-R. Pérez-Núñez, C. Rodríguez, L.-J. Vásquez-Serpa, and C. Navarro, "The Challenge of Deep Learning for the Prevention and Automatic Diagnosis of Breast Cancer: A Systematic Review," *Diagnostics*, vol. 14, no. 24, p. 2896, Dec. 2024, doi: 10.3390/diagnostics14242896.

[41] M. Harishbhai Tilala *et al.*, "Ethical Considerations in the Use of Artificial Intelligence and Machine Learning in Health Care: A Comprehensive Review," *Cureus*, Jun. 2024, doi: 10.7759/cureus.62443.

[42] Gold Nmesoma Okorie, Chioma Ann Udeh, Ejuma Martha Adaga, Obinna Donald DaraOjimba, and Osato Itohan Oriekhoe, "ETHICAL CONSIDERATIONS IN DATA COLLECTION AND ANALYSIS: A REVIEW: INVESTIGATING ETHICAL PRACTICES AND CHALLENGES IN MODERN DATA COLLECTION AND ANALYSIS," *Int. J. Appl. Res. Soc. Sci.*, vol. 6, no. 1, pp. 1–22, Jan. 2024, doi: 10.51594/ijarss.v6i1.688.

[43] A. Srivastava, R. Sharma, and R. Srivastava, "Ethical Data Management in Healthcare Industry," 2024, Accessed: Jan. 02, 2025. [Online]. Available: http://article.sapub.org/10.5923.j.ajmms.20241412.11.html

[44] R. Margam, "Ethics And Data Privacy: The Backbone of Trustworthy Healthcare Practices," Nov. 2023, doi: 10.59535/sehati.v1i2.115.

[45] S. Tosoni *et al.*, "The use of personal health information outside the circle of care: consent preferences of patients from an academic health care institution," *BMC Med. Ethics*, vol. 22, no. 1, p. 29, Dec. 2021, doi: 10.1186/s12910-021-00598-3.

[46] S. Huda, Md. R. Islam, J. Abawajy, V. N. V. Kottala, and S. Ahmad, "A Cyber Risk Assessment Approach to Federated Identity Management Framework-Based Digital Healthcare System," *Sensors*, vol. 24, no. 16, p. 5282, Aug. 2024, doi: 10.3390/s24165282.

[47] 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.

[48] M. Mahmood *et al.*, "Addressing Security Issues, Threats,Attacks and Challenges to Improve the Security Architecture of Internet of Medical Things," pp. 974–8571, Jun. 2022.

[49] S. Madanian, T. Chinbat, M. Subasinghage, D. Airehrour, F. Hassandoust, and S. Yongchareon, "Health IoT Threats: Survey of Risks and Vulnerabilities," *Future Internet*, vol. 16, no. 11, p. 389, Oct. 2024, doi: 10.3390/fi16110389.

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

[51] V. Chiruvella and A. K. Guddati, "Ethical Issues in Patient Data Ownership," *Interact. J. Med. Res.*, vol. 10, no. 2, p. e22269, May 2021, doi: 10.2196/22269.

[52] N. Khalid, A. Qayyum, M. Bilal, A. Al-Fuqaha, and J. Qadir, "Privacy-preserving artificial intelligence in healthcare: Techniques and applications," *Comput. Biol. Med.*, vol. 158, p. 106848, May 2023, doi: 10.1016/j.compbiomed.2023.106848.

[53] N. N. Basil, S. Ambe, C. Ekhator, and E. Fonkem, "Health Records Database and Inherent Security Concerns: A Review of the Literature," *Cureus*, Oct. 2022, doi: 10.7759/cureus.30168.

[54] S. M. Williamson and V. Prybutok, "Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare," *Appl. Sci.*, vol. 14, no. 2, p. 675, Jan. 2024, doi: 10.3390/app14020675.

[55] S. A. Alowais *et al.*, "Revolutionizing healthcare: the role of artificial intelligence in clinical practice," *BMC Med. Educ.*, vol. 23, no. 1, p. 689, Sep. 2023, doi: 10.1186/s12909-023-04698-z.

[56] H. Andersson, A. Svensson, C. Frank, A. Rantala, M. Holmberg, and A. Bremer, "Ethics education to support ethical competence learning in healthcare: an integrative systematic review," *BMC Med. Ethics*, vol. 23, no. 1, p. 29, Dec. 2022, doi: 10.1186/s12910-022-00766-z.

[57] Oluwatosin Ilori, Tolulope Olagoke Kolawole, and Janet Aderonke Olaboye, "Ethical dilemmas in healthcare management: A comprehensive review," *Int. Med. Sci. Res. J.*, vol. 4, no. 6, pp. 703–725, Jun. 2024, doi: 10.51594/imsrj.v4i6.1251.

[58] B. Adhikari, C. Pell, and P. Y. Cheah, "Community engagement and ethical global health research," *Glob. Bioeth.*, vol. 31, no. 1, pp. 1–12, Jan. 2020, doi: 10.1080/11287462.2019.1703504.

[59] T. Rong, E. Ristevski, and M. Carroll, "Exploring community engagement in place-based approaches in areas of poor health and disadvantage: A scoping review," *Health Place*, vol. 81, p. 103026, May 2023, doi: 10.1016/j.healthplace.2023.103026.

[60] S. Nabukenya, D. Kyaddondo, I. G. Munabi, C. Waitt, A. Twimukye, and E. S. Mwaka, "The role of community engagement in promoting research participants' understanding of pharmacogenomic research results: Perspectives of stakeholders involved in HIV/AIDS research and treatment," *PLOS ONE*, vol. 19, no. 4, p. e0299081, Apr. 2024, doi: 10.1371/journal.pone.0299081.

[61] H. Alderwick, A. Hutchings, A. Briggs, and N. Mays, "The impacts of collaboration between local health care and non-health care organizations and factors shaping how they work: a systematic review of reviews," *BMC Public Health*, vol. 21, no. 1, p. 753, Apr. 2021, doi: 10.1186/s12889-021-10630-1.

[62] M. W. Kreuter, T. Thompson, A. McQueen, and R. Garg, "Addressing Social Needs in Health Care Settings: Evidence, Challenges, and Opportunities for Public Health," *Annu. Rev. Public Health*, vol. 42, no. 1, pp. 329–344, Apr. 2021, doi: 10.1146/annurev-publhealth-090419-102204.