Technoarete Transactions on Advances in Data Science and Analytics
Vol-3, Issue-1, February 2024
e-ISSN: 2583-2956

Deciphering the Digital Healthscape: Unveiling the Intricacies of the Internet of Medical Things (IoMT)

Gulafshan Ara[1*], Md. Masroor Ahmed[2], Rajeev Kumar[3], Arif Md. Sattar[4], Mritunjay Kr. Ranjan[5]

[1] Research Scholar, P.G. Department of Mathematics and Computer Science, Magadh University, Bodh, Gaya, Bihar, India
[2] Associate Professor, Department of Physics, Mirza Ghalib College, Gaya, Bihar, India
[3] Professor, Department of MCA, Diwan V.S. Institute of Management Studies, Meerut, Uttar Pradesh, India
[4] Associate Professor, Diwan V.S. Institute of Management Studies, Meerut, Uttar Pradesh, India
[5] Assistant Professor, School of Computer Science and Engineering Sandip University, Nashik, Maharashtra, India
Corresponding Author Email: abbassahiba1996@gmail.com

Abstract

Through the integration of networking, data analytics, and medical devices, the Internet of Medical Things (IoMT) has revolutionized patient care and healthcare administration. Presented here is extensive study on IoMT that sheds light on its impact on healthcare settings, including its origins, technical foundations, uses, security worries, interoperability problems, and potential future developments. The evolution of IoMT began with the integration of internet connection with medical devices and continues with the complex and linked environment of today. This shift in thinking makes possible preventative healthcare, individualized treatment plans, and remote patient monitoring. Technologies for data storage, networking, and sensors are the backbone of IoMT. Streamlined connection, real-time data transmission, and a robust IoMT architecture for healthcare applications are all described in the article. Remote patient monitoring and the management of chronic illnesses are two areas where IoMT finds application in healthcare. Literature show how IoMT describes a data-driven, proactive, and personalized healthcare delivery strategy that improves patient outcomes, treatment adherence, and resource utilization. The research addresses important topics related to IoMT, such as healthcare privacy and security. Securing IoMT and bolstering trust in connected healthcare are the goals of research into encryption, access controls, and data protection regulations. To implement IoMT, interoperability concerns must be addressed. The essay delves into the difficulties of integrating IoMT devices and systems, as well as the necessity of standardized frameworks to facilitate data sharing and interoperability. Future advances in the IoMT, such as the integration of AI and blockchain for security, are predicted in the research. The paper highlights the potential of IoMT to impact healthcare delivery and address global healthcare concerns. This study demonstrates the transformation of IoMT to academics, healthcare professionals, and policymakers.

Keywords

Internet of Medical Things (IoMT), Digital Healthscape, Remote Patient Monitoring, Data Analytics, Security, Interoperability, Future Trends.

INTRODUCTION

The implementation of novel technologies has brought about a significant transformation in the healthcare sector, with the Internet of Medical Things (IoMT) converging as a leading in this outstanding age. IoMT is challenging long-held beliefs regarding the delivery of healthcare by ushering in a new era of proactive, individualized, and networked medical services [1]. The aforementioned goal is being accomplished by integrating data analytics, medical apparatus, and networking infrastructure. The objective of this all-encompassing analysis is to resolve the enigmas associated with the IoMT through an investigation of its inception, structure, healthcare implementations, security considerations, challenges in interoperability, and prospective advancements. The trajectory of the Internet of Things (IoMT) during its infancy constitutes a pivotal element in its historical account. We progressed from a simple connection to a complex link ecology by following this path. IoMT has evolved from its early stages as a network that linked medical devices to the internet to become a dynamic network that facilitates remote monitoring, real-time data exchange, and enhanced healthcare treatments [2]. For the purpose of situating IoMT and foreseeing potential future developments, it is critical to possess a comprehensive comprehension of its evolutionary trajectory. The concept of "the Internet of Things" (IoMT) is defined by its technical foundations. Sensor technology, data storage systems, and protocols for device interoperability comprise these foundations. The formation of the Internet of Medical Things (IoMT) requires the collaboration and integration of this collection of elements. Their ability to facilitate remote patient monitoring and make valuable contributions to data-driven healthcare solutions is undeniably remarkable. Furthermore, they furnish healthcare providers with up-to-date information. We must examine these technical foundations attentively if we are to comprehend how IoMT operates and what its revolutionary effects will be in healthcare. Medical equipment that is connected to the IoMT may provide advantages for various healthcare applications. Potential medical applications for these technologies include individualized medication, remote patient monitoring, and the management of chronic diseases. The literature and case studies demonstrate that the IoMT is facilitating patient empowerment in healthcare decision-making and enhancing treatment efficacy. Treatment modifications for patients are also discernible. The purpose of this research is to conduct a

e-ISSN: 2583-2956

comprehensive evaluation of these applications so that patients and medical professionals can comprehend the true benefits of IoMT. As a result, we shall possess the ability to elucidate their merits. IoMT-presented opportunities for transformation are not devoid of obstacles, however [3]. Extra safeguards need to be put in place to keep patients' private health information safe because security and privacy breaches happen so often in the healthcare field. Interoperability issues are an additional hinderance to the seamless integration of numerous IoMT devices and systems. This research further explores these concerns and presents results regarding possible remedies and approaches to guarantee the appropriate and protected implementation of IoMT in healthcare establishments. With a deeper exploration of IoMT, we trust that you will acquire a more comprehensive comprehension of this technological revolution and its ramifications, challenges, and prospective avenues for growth within the ever-evolving domain of contemporary healthcare. Academics, policymakers, healthcare professionals, and IT enthusiasts are all invited to partake in the study's discoveries concerning the ever-evolving Internet of Medical Things.

Objective:

a. To analyze the current landscape of digital health technologies, focusing on the IoMT, to identify key trends, challenges, and opportunities.
b. To explore the interconnectedness and interoperability of IoMT devices and systems, aiming to understand their potential impact on healthcare delivery, patient outcomes, and data security.
c. To evaluate regulatory and ethical concerns in IoMT adoption, providing guidance for policymakers, healthcare professionals, and industry stakeholders to navigate challenges.

RELATED STUDY

The Internet of Things has transformed the healthcare sector by enabling the smooth incorporation of medical equipment, data analysis, and artificial intelligence. Consequently, patient care is enhanced, leading to improved clinical results. Numerous recent investigations have explored the complexities of IoMT and its influence on contemporary healthcare frameworks.

The authors delved into the intersection of medical data analysis, artificial intelligence (AI), and the Internet of Medical Things in their research article featured in Bioengineering [4]. Through the fusion of sophisticated data analytics methods with the capabilities of AI and IoMT devices, the scholars underscored the opportunity for transforming healthcare provision and personalized medicine. The research underscores the significance of utilizing data-driven perspectives to inform consequential healthcare choices, consequently enhancing patient results.

Conducted a comparative analysis focusing on the integration of artificial intelligence and the Internet of Medical Things for medical decision support systems. Presented in Lecture Notes in Networks and Systems, their study underscores the synergies between AI technologies and IoMT devices in facilitating informed medical decisions [5]. By comparing various approaches, the researchers shed light on the transformative role of AI-IoMT integration in optimizing clinical workflows, enhancing diagnostic accuracy, and improving patient care.

In a bibliometric analysis that was published in [6], the researchers have presented valuable insights regarding the trends and progressions within the realm of Medical Internet of Things (MIoT) for contemporary healthcare. Through a thorough examination of the current body of literature, the study presents a detailed outline of the research environment, emphasizing significant advancements, obstacles, and prospective pathways in utilizing MIoT technologies to transform healthcare delivery.

Examined in this study is the evolution of the Internet of Medical Things sector in China, as delineated in the publication entitled "Frontiers in Artificial Intelligence and Applications" [7]. A comprehensive analysis is presented, delving into the developmental stage and future projections of the IoMT industry in China. This research offers profound insights into the market trends, technological advancements, and regulatory framework that are influencing the landscape of the IoMT domain within the region.

The fundamental framework supporting the Internet of Medical Things (IoMT) serves as a crucial backbone enabling the smooth integration of healthcare devices, connectivity, and data interpretation in the medical field. These core elements work together harmoniously to empower the IoMT environment in efficiently collecting, sending, and analyzing health data in real-time. Delve below lies a comprehensive exploration of the technological foundations of IoMT.

COMPONENTS

Wearable devices, RPM systems, medical sensors, mobile health applications, cloud technology, data analysis, communication standards, and infrastructure combine to form the intricate network of technologies that constitute the Internet of Medical Things (IoMT). The ability of this all-encompassing system to collect, transmit, and interpret health information enables remote patient monitoring, personalized healthcare services, and proactive disease control. A comprehensive understanding of these elements is essential for effectively navigating the IoMT environment. Key considerations include ethical implications, security protocols, compatibility, and performance. Exploring this subject allows stakeholders to gain insights into the transformative impact of IoMT technologies on healthcare provision, patient engagement, and advancements in digital health (Table 1).

e-ISSN: 2583-2956

Table 1. Components of IoMT with its subcomponents and work

Citation	Components	Sub-components	Work
[9]	Sensors and Devices	Miniaturization	Advancements in sensor technologies have led to the miniaturization of medical sensors, allowing for unobtrusive integration into various wearable devices and medical equipment.
		Biometric Sensors	Specialized biometric sensors, such as heart rate monitors, blood pressure sensors, and glucose monitors, provide real-time data on patients' physiological parameters.
		Environmental Sensors	Integration of environmental sensors for monitoring factors like temperature, humidity, and air quality in healthcare settings.
[10]	Communication Protocols	Wireless Technologies	Utilization of wireless communication protocols, including Bluetooth, Wi-Fi, and Zigbee, facilitates seamless connectivity between IoMT devices and the broader healthcare infrastructure.
		Low-Power Protocols	Low-power communication protocols enhance energy efficiency in IoMT devices, extending battery life and ensuring continuous monitoring over extended periods.
[11]	Data Storage and Transmission	Cloud Computing	Integration with cloud computing allows for centralized storage and processing of vast amounts of health data, enabling scalability, accessibility, and collaborative data analysis.
		Edge Computing	Utilization of edge computing to process data closer to the source, reducing latency and ensuring timely analysis of critical health information.
		Secure Data Transmission	Implementation of secure data transmission protocols, such as encryption and secure sockets layer (SSL), to protect patient information during data transfer.
[12]	Interoperability Standards	Healthcare Standards	Adoption of healthcare interoperability standards, such as Health Level Seven International (HL7) and Fast Healthcare Interoperability Resources (FHIR), to ensure seamless communication between different healthcare systems and IoMT devices.
		Device Integration Protocols	Implementation of standardized protocols for device integration, promoting interoperability between diverse IoMT devices from different manufacturers.
[13]	User Interfaces and Experience	Human-Machine Interaction	Development of user-friendly interfaces to enhance the interaction between healthcare professionals, patients, and IoMT devices.
		Mobile Applications	Integration with mobile applications for convenient data visualization, patient engagement, and remote monitoring.
[14]	Security Measures	Data Encryption	Robust data encryption techniques to protect sensitive health information from unauthorized access during transmission and storage.
		Authentication and Authorization	Implementation of secure authentication and authorization mechanisms to ensure that only authorized personnel can access IoMT data.
[15]	Artificial Intelligence (AI) Integration	Machine Learning Algorithms	Integration of machine learning algorithms to analyze large datasets, identify patterns, and provide predictive insights for personalized healthcare.
		Decision Support Systems	Development of AI-driven decision support systems that assist healthcare professionals in clinical decision-making based on real-time patient data.

Understanding these technological foundations is crucial for comprehending how IoMT operates and evolves. The synergy of these elements forms the backbone of IoMT, empowering healthcare professionals with valuable insights and contributing to the transformation of healthcare deliver.

e-ISSN: 2583-2956

APPLICATIONS IN HEALTHCARE

The applications of the Internet of Medical Things (IoMT) in healthcare are diverse and transformative, offering innovative solutions to improve patient care, enhance disease management, and optimize healthcare delivery. IoMT leverages interconnected devices, real-time data exchange, and advanced analytics to revolutionize various aspects of healthcare. Here is a detailed exploration of the applications of IoMT in healthcare in (Table.2).

Table 2. IoMT Technology and Benefits

Citation	Technology	Benefits
[16]	Remote Patient Monitoring	Facilitates proactive healthcare management, early detection of anomalies, and timely interventions for individuals with chronic conditions or those recovering from surgeries.
[17]	Chronic Disease Management	Enhances treatment adherence, allows for timely adjustments to treatment plans, and reduces the frequency of hospital visits.
[18]	Personalized Medicine	Optimizes treatment efficacy, minimizes adverse effects, and ensures a more targeted approach to patient care
[19]	Preventive Healthcare	Encourages a shift from reactive to proactive healthcare, focusing on wellness and prevention, ultimately reducing the burden on the healthcare system.
[20]	Medication Adherence	Improves medication adherence, reduces the risk of medication errors, and enhances overall treatment outcomes.
[21]	Smart Healthcare Environments	Optimizes resource utilization, improves workflow efficiency, and enhances the overall quality of patient care.
[22]	Emergency Response Systems	Enables rapid response to critical health events, reducing response time and improving outcomes in emergency situations.
[23]	Rehabilitation and Physical Therapy	Enhances the effectiveness of rehabilitation programs, enables remote monitoring of patient progress, and facilitates personalized rehabilitation plans.
[24]	Clinical Trials and Research	Accelerates the pace of medical research, enables more efficient recruitment for clinical trials, and enhances the generalizability of research findings.
[25]	Patient Engagement and Empowerment	Empowers patients to actively participate in their healthcare, promotes informed decision-making, and strengthens the patient-provider relationship.

These applications collectively demonstrate the transformative impact of IoMT on healthcare, offering a paradigm shift towards more personalized, efficient, and patient-centric approaches to medical care. As technology continues to advance, the potential for IoMT to further revolutionize healthcare remains vast.

SECURITY AND PRIVACY

While there are many positive outcomes from healthcare organisations implementing IoMT, there are also many negative outcomes related to privacy and security [26]. Keeping people's faith in IoMT systems depends on making sure sensitive health data is available, secure, and kept confidential at all times. This article delves deeply into the privacy and security issues surrounding IoMT.

Table 3. IoMT, Security and privacy with respect to its properties and mitigation

Citation	Properties	Concern	Mitigation
[27]	Data Breaches and Unauthorize-d Access	IoMT systems generate and transmit vast amounts of sensitive health data. Unauthorized access or data breaches can lead to the exposure of patients' personal information, medical history, and treatment plans.	Robust access controls, encryption, and authentication mechanisms are crucial to preventing unauthorized access. Regular security audits and vulnerability assessments help identify and address potential weaknesses.
[28]	Data Integrity	Tampering with health data, either intentionally or unintentionally, can compromise the accuracy of medical records, leading to incorrect diagnoses or treatment decisions.	Implementing data integrity checks, cryptographic hashes, and ensuring secure data transmission can help safeguard against data tampering.

e-ISSN: 2583-2956

Citation	Properties	Concern	Mitigation
[29]	Interoperabil-ity Challenges	The diverse nature of IoMT devices and systems can create challenges in achieving seamless interoperability. Incompatibilities between devices may introduce vulnerabilities and hinder secure data exchange.	Adhering to standardized communication protocols, such as HL7 and FHIR, can enhance interoperability. Regular updates and patches to address security vulnerabilities should be implemented.
[30]	Device Security	IoMT devices, especially those connected to the internet, are susceptible to cyber-attacks. Compromised devices can be used to gain unauthorized access to healthcare networks or launch attacks on other connected devices.	Implementing strong device authentication, regular software updates, and network segmentation can enhance the security of IoMT devices.
[31]	Data Encryption and Transmission	Unencrypted data transmission poses a significant risk as intercepted data may be vulnerable to eavesdropping or man-in-the-middle attacks.	Utilizing strong encryption algorithms for data in transit, such as SSL/TLS, ensures secure communication between IoMT devices and backend systems.
[32]	Patient Consent and Data Ownership	Determining the ownership of health data and obtaining informed patient consent for data sharing are ethical and legal considerations that must be addressed to protect patient rights.	Establishing clear policies on data ownership, informed consent processes, and adherence to data protection regulations ensures transparency and respects patient privacy.
[33]	Regulatory Compliance	Non-compliance with data protection regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, can result in legal consequences and erode patient trust.	Adhering to relevant healthcare regulations, regularly conducting compliance audits, and adopting privacy by design principles are essential for maintaining regulatory compliance.
[34]	Supply Chain Security	Ensuring the security of the entire IoMT supply chain, from device manufacturing to deployment, is crucial. Weaknesses at any stage may be exploited by malicious actors.	Collaborating with reputable vendors, performing security assessments on devices, and maintaining visibility into the entire supply chain help mitigate potential security risks.
[35]	Data Residency and Storage	Storage of health data in cloud environments raises questions about data residency, jurisdictional compliance, and the potential exposure of sensitive information to third-party entities.	Implementing clear data residency policies, encrypting stored data, and choosing cloud service providers with robust security measures help address concerns related to data storage.
[36]	Educational and Awareness Gaps	Insufficient education and awareness among healthcare professionals, patients, and device manufacturers about cybersecurity practices and risks may lead to inadvertent security lapses.	Providing comprehensive training programs, raising awareness about cybersecurity best practices, and fostering a culture of security across the healthcare ecosystem contribute to addressing educational gaps.

A comprehensive strategy incorporating organisational, regulatory, and technology components is necessary to resolve these privacy and security issues. Strong security measures must be put in place to protect patient information and keep healthcare systems running smoothly as IoMT develops further.

INTEROPERABILITY CHALLENGES

The challenges of interoperability pose a significant obstacle to the smooth integration and operation of the IoMT in the healthcare sector [37]. Given the involvement of numerous devices, systems, and platforms in IoMT, it is crucial to provide efficient communication and coordination across these components (Table. 4).

e-ISSN: 2583-2956

Table 4. Interoperability challenges associated with IoMT.

Citation	Attributes	Challenge	Mitigation
[38]	Diverse Standards and Protocols	IoMT encompasses a wide array of devices and systems, each often operating on different communication protocols and standards. This diversity can hinder the smooth exchange of data between devices and platforms.	Adopting standardized communication protocols, such as HL7, FHIR, or DICOM, promotes uniformity and facilitates interoperability among diverse IoMT components.
[39]	Lack of Standardization in Data Formats	Variation in data formats and structures used by different IoMT devices may lead to difficulties in interpreting and integrating data, impeding the seamless flow of information.	Establishing standardized data formats and structures ensures consistency, making it easier for different IoMT devices and systems to understand and interpret shared data.
[40]	Data Silos and Fragmentation	IoMT implementations often result in data silos where information is compartmentalized and not easily accessible across different healthcare systems or platforms.	Implementing interoperability standards and utilizing data exchange frameworks help break down silos, allowing for a more unified view of patient information.
[41]	Vendor-Specific Solutions	Some IoMT devices and platforms are developed by different vendors, each with its proprietary solutions. This can lead to compatibility issues and hinder interoperability.	Encouraging vendors to adopt open standards and participate in interoperability initiatives facilitates collaboration and ensures compatibility across a diverse IoMT ecosystem.
[42]	Resistance to Change	Resistance to change within healthcare organizations and among healthcare professionals can hinder the successful adoption and integration of IoMT technologies.	Implementing change management strategies, fostering a culture of innovation, and emphasizing the benefits of IoMT adoption can help overcome resistance and facilitate interoperability.

To overcome these issues with compatibility, it is necessary for healthcare participants, technology creators, and regulatory organisations to work together in a cooperative manner. To fully leverage the benefits of IoMT for enhanced patient care and healthcare efficiency, the healthcare industry should prioritise standardisation, data security, and interoperability.

FUTURE DIRECTIONS

Patients can anticipate better outcomes, new obstacles, and a complete overhaul of healthcare delivery with the advent of the IoMT. Some important developments include the following: the rise of AI, improvements in RPM, 5G connectivity, edge computing for real-time data processing, the Internet of Medical Things (IoMT) playing a larger role in global health initiatives, better personalisation with IoMT analytics, and the creation of interoperability standards and frameworks. IoMT devices will improve real-time analytics by processing data closer to its source using edge computing capabilities, which will decrease latency. When it comes to managing disasters and responding to pandemics, IoMT will be an essential tool. Healthcare interventions, therapy programmes, and medication schedules that are tailored to each individual will also benefit from IoMT. Initiatives related to IoMT must prioritise ethical concerns, patient empowerment, and long-term viability. To successfully traverse these future routes, it is crucial that healthcare experts, tech developers, lawmakers, and regulatory agencies work together. The healthcare industry can transform patient care, enhance health outcomes, and boost efficiency in the healthcare system by fully embracing these trends and realising the potential of IoMT.

CONCLUSION

The analysis of the Internet of Medical Things (IoMT) showcases a landscape defined by innovation, transformative potential, and challenges. The evolution of IoMT underscores its significant impact on healthcare delivery, transitioning from basic medical device integration to a sophisticated ecosystem. The technological foundations, encompassing sensors, communication protocols, and data analytics, form the core of IoMT applications. Its use in healthcare, from remote patient monitoring to personalized medicine, signals a shift towards data-driven, patient-centric solutions. While IoMT has demonstrated positive outcomes in patient care, challenges such as security, privacy, and interoperability require attention through standardized frameworks and collaborative efforts. The future of IoMT holds promise with AI integration, remote monitoring advancements, blockchain security, and 5G connectivity shaping innovation.

e-ISSN: 2583-2956

Emphasizing ethical considerations, user experience, and sustainability will be crucial in responsible technology deployment. Collaboration among stakeholders will be essential in realizing IoMT's full potential, fostering adaptability, transparency, and patient empowerment for a more efficient and patient-centric healthcare ecosystem.

REFERENCES

[1] B. Sharma, D. Kaushal, M. Sharma, S. Joshi, S. Gopal, and P. Gupta, "Integration of AI, Digital Twin and Internet of Medical Things (IoMT) For Healthcare 5.0: A Bibliometric Analysis," Nov. 2023, doi: https://doi.org/10.1109/icaiccit60255.2023.10466141.

[2] Z. Zhou, "Design of medical equipment integrated management system based on Internet of Things," Mar. 2022, doi: https://doi.org/10.1109/icitbs55627.2022.00092.

[3] S. F. Ahmed, M. 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," Information Fusion, p. 102060, Sep. 2023, doi: https://doi.org/10.1016/j.inffus.2023.102060.

[4] M. Diwakar, P. Singh, and V. Ravi, "Medical Data Analysis Meets Artificial Intelligence (AI) and Internet of Medical Things (IoMT)," Bioengineering, vol. 10, no. 12, p. 1370, Nov. 2023, doi: https://doi.org/10.3390/bioengineering10121370.

[5] Asma Merabet, Asma Saighi, and Zakaria Laboudi, "Artificial Intelligence and Internet of Medical Things for Medical Decision Support Systems: Comparative Analysis," Lecture notes in networks and systems, pp. 134–140, Jan. 2023, doi: https://doi.org/10.1007/978-3-031-44146-2_14.

[6] H.-S. Nguyen et al., "A Bibliometrics Analysis of Medical Internet of Things for Modern Healthcare," Electronics, vol. 12, no. 22, p. 4586, Jan. 2023, doi: https://doi.org/10.3390/electronics12224586.

[7] H.-S. Nguyen et al., "A Bibliometrics Analysis of Medical Internet of Things for Modern Healthcare," Electronics, vol. 12, no. 22, p. 4586, Jan. 2023, doi: https://doi.org/10.3390/electronics12224586.

[8] A. Sobecki, J. Szymanski, D. Gil, and H. Mora, "Framework for Integration Decentralized and Untrusted Multi-vendor IoMT Environments," IEEE Access, pp. 1–1, 2020, doi: https://doi.org/10.1109/access.2020.3000636.

[9] I. Rodríguez-Rodríguez, M. Campo-Valera, and J.-V. Rodríguez, "Forecasting glycaemia for type 1 diabetes mellitus patients by means of IoMT devices," Internet of Things, vol. 24, p. 100945, Dec. 2023, doi: https://doi.org/10.1016/j.iot.2023.100945.

[10] C.-M. Chen, S. Liu, X. Li, S. H. Islam, and A. K. Das, "A provably-secure authenticated key agreement protocol for remote patient monitoring IoMT," Journal of Systems Architecture, vol. 136, p. 102831, Mar. 2023, doi: https://doi.org/10.1016/j.sysarc.2023.102831.

[11] A. Melnyk, Y. Morozov, Bohdan Havano, and Petro Hupalo, "Protection of Biometric Data Transmission and Storage in the Human State Remote Monitoring Tools," 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Sep. 2021, doi: https://doi.org/10.1109/idaacs53288.2021.9661047.

[12] A. Talaminos-Barroso, J. Reina-Tosina, and L. M. Roa, "Adaptation and application of the IEEE 2413-2019 standard security mechanisms to IoMT systems," Measurement: Sensors, vol. 22, p. 100375, Aug. 2022, doi: https://doi.org/10.1016/j.measen.2022.100375.

[13] R. Dwivedi, D. Mehrotra, and S. Chandra, "Potential of internet of medical things (IOMT) applications in building a smart healthcare system: A systematic review," Journal of Oral Biology and Craniofacial Research, vol. 12, no. 2, Dec. 2021, doi: https://doi.org/10.1016/j.jobcr.2021.11.010.

[14] A. Talaminos-Barroso, J. Reina-Tosina, and L. M. Roa, "Adaptation and application of the IEEE 2413-2019 standard security mechanisms to IoMT systems," Measurement: Sensors, vol. 22, p. 100375, Aug. 2022, doi: https://doi.org/10.1016/j.measen.2022.100375.

[15] A. Mittal, L. Dumka, and L. Mohan, "A Comprehensive Review on the Use of Artificial Intelligence in Mental Health Care," Jul. 2023, doi: https://doi.org/10.1109/icccnt56998.2023.10308255.

[16] M. W. Condry and Xiaohong Iris Quan, "Remote Patient Monitoring Technologies and Markets," pp. 1–5, Jan. 2023, doi: https://doi.org/10.1109/emr.2023.3285688.

[17] K. S. Adewole et al., "Cloud-based IoMT framework for cardiovascular disease prediction and diagnosis in personalized E-health care," pp. 105–145, Jan. 2021, doi: https://doi.org/10.1016/b978-0-12-821187-8.00005-8.

[18] D. Padmavilochanan et al., "Personalized diabetes monitoring platform leveraging IoMT and AI for non-invasive estimation," Smart Health, p. 100428, Sep. 2023, doi: https://doi.org/10.1016/j.smhl.2023.100428.

[19] A. Koren and R. Prasad, "Internet of Things: Shaping Healthcare during COVID-19 Pandemic," Dec. 2021, doi: https://doi.org/10.1109/wpmc52694.2021.9700472.

[20] K. Gorman, Ilia Ratsev, L. Lu, and Casey Overby Taylor, "An Interactive Visualization Tool for Medication (Re)fill Adherence: A Case Study of Pharmacy Claims-derived Adherence Measures in Asthmatics," 2022 IEEE 10th International Conference on Healthcare Informatics (ICHI), Jun. 2022, doi: https://doi.org/10.1109/ichi54592.2022.00044.

[21] S. Rani, A. Kataria, S. Kumar, and P. Tiwari, "Federated learning for secure IoMT-applications in smart healthcare systems: A comprehensive review," Knowledge-Based Systems, p. 110658, May 2023, doi: https://doi.org/10.1016/j.knosys.2023.110658.

[22] Khosro Rezaee et al., "IoMT-Assisted Medical Vehicle Routing Based on UAV-Borne Human Crowd Sensing and Deep Learning in Smart Cities," IEEE Internet of Things Journal, vol. 10, no. 21, pp. 18529–18536, Nov. 2023, doi: https://doi.org/10.1109/jiot.2023.3284056.

[23] A. Buzachis, Giuseppe Massimo Bernava, M. Busa, G. Pioggia, and M. Villari, "Towards the Basic Principles of Osmotic Computing: A Closed-Loop Gamified Cognitive Rehabilitation Flow Model," Oct. 2018, doi: https://doi.org/10.1109/cic.2018.00067.

[24] Hafiz Muhammad Zeeshan et al., "Worldwide Research Trends and Hotspot on IOMT Based on Bibliometric Analysis," Dec. 2023, doi: https://doi.org/10.1109/iccwamtip60502.2023.10387075.

[25] E. Mbunge et al., "Framework for ethical and acceptable use of social distancing tools and smart devices during COVID-19 pandemic in Zimbabwe," Sustainable Operations and Computers, vol. 2, pp. 190–199, 2021, doi: https://doi.org/10.1016/j.susoc.2021.07.003.

e-ISSN: 2583-2956

[26] Z. A. Solangi, Y. A. Solangi, S. Chandio, M. bt. S. Abd. Aziz, M. S. bin Hamzah, and A. Shah, "The future of data privacy and security concerns in Internet of Things," 2018 IEEE International Conference on Innovative Research and Development (ICIRD), May 2018, doi: https://doi.org/10.1109/icird.2018.8376320.

[27] S. F. Ahmed, M. 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," Information Fusion, p. 102060, Sep. 2023, doi: https://doi.org/10.1016/j.inffus.2023.102060.

[28] 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 of Things, vol. 23, p. 100887, Oct. 2023, doi: https://doi.org/10.1016/j.iot.2023.100887.

[29] G. Yasmeen, N. Javed, and T. Ahmed, "Interoperability: A Challenge for IoMT," ECS Transactions, vol. 107, no. 1, pp. 4459–4467, Apr. 2022, doi: https://doi.org/10.1149/10701.4459ecst.

[30] S. Lee, Eun Kwang Lee, Byung Chul Jang, and H. Yoo, "Hardware-based security devices using a physical unclonable function created by the irregular grain boundaries found in perovskite calcium titanate," Journal of Alloys and Compounds, vol. 969, pp. 172329–172329, Dec. 2023, doi: https://doi.org/10.1016/j.jallcom.2023.172329.

[31] S. Shivananda, M. Sathya, K. Janani, and U. Arunkumar, "DNN and Cryptography based Data Monitoring System for IoMT Environment," Nov. 2023, doi: https://doi.org/10.1109/icscna58489.2023.10370190.

[32] Deepak Kumar Mishra and Pawan Singh Mehra, "Blockchain-based Patient-Centric Healthcare Architecture: A Secure and Efficient Approach for Medical Data Sharing," Jul. 2023, doi: https://doi.org/10.1109/icccnt56998.2023.10307004.

[33] P. R. S, Abdul Haq Nalband, Sachin U, Chaithanya V, and Mohammed Riyaz Ahmed, "Securing 5G-Enabled Internet of Medical Things in Healthcare: Vulnerabilities, Threats, and Architectural Framework," Nov. 2023, doi: https://doi.org/10.1109/csitss60515.2023.10334074.

[34] C. Wang and H. Zhang, "Construction of Supply Chain Security Management Model for Information and Communication Technology Based on the Internet of Things and Cloud Computing," Procedia Computer Science, vol. 228, pp. 745–754, Jan. 2023, doi: https://doi.org/10.1016/j.procs.2023.11.088.

[35] Kapil Singi, Kanchanjot Kaur Phokela, Narendranath Sukhavasi, and Vikrant Kaulgud, "Framework for Recommending Data Residency Compliant Application Architecture," Dec. 2021, doi: https://doi.org/10.1109/apsec53868.2021.00065.

[36] P. Goyal, T. Kukreja, A. Agarwal, and N. Khanna, "Narrowing awareness gap by using e-learning tools for counselling university entrants," IEEE Xplore, Mar. 01, 2015. https://ieeexplore.ieee.org/document/7164822 (accessed Mar. 16, 2023).

[37] Fadi Muheidat and L. A. Tawalbeh, "AIoMT artificial intelligence (AI) and Internet of Medical Things (IoMT)," Elsevier eBooks, pp. 33–54, Jan. 2023, doi: https://doi.org/10.1016/b978-0-323-99421-7.00013-1.

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

[39] J. Gao, L. Lei, and S. Yu, "Big Data Sensing and Service: A Tutorial," Mar. 2015, doi: https://doi.org/10.1109/bigdataservice.2015.45.

[40] R. Hai et al., "Amalur: Data Integration Meets Machine Learning," arXiv (Cornell University), Apr. 2023, doi: https://doi.org/10.1109/icde55515.2023.00301.

[41] J. M. T. I. Jayalath, E. J. A. P. C. Chathumali, K. R. M. Kothalawala, and N. Kuruwitaarachchi, "Green Cloud Computing: A Review on Adoption of Green-Computing attributes and Vendor Specific Implementations," 2019 International Research Conference on Smart Computing and Systems Engineering (SCSE), Mar. 2019, doi: https://doi.org/10.23919/scse.2019.8842817.

[42] N. Hajiheydari, M. S. Delgosha, and H. Olya, "Scepticism and resistance to IoMT in healthcare: Application of behavioural reasoning theory with configurational perspective," Technological Forecasting and Social Change, vol. 169, p. 120807, Aug. 2021, doi: https://doi.org/10.1016/j.techfore.2021.120807.