Current Journal of Engineering and Science Research
Volume 2, Issue 8, pp 24-28, August 2025
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2025.208005
Available Online at https://www.cjesr.com

Next-Generation Embedded Systems for IoMT: Design Constraints and Opportunities

[1]Dewi Kartika, [2]Fajar Hidayat, [3]Arif Wijaya, [4]Siti Wulandari

[1,2,3]Specialized in Electronics and Engineering Technology, Oliteknik Elektronika Negeri Surabaya (PENS), Indonesia

Abstract: The Internet of Medical Things (IoMT) is transforming the healthcare sector through the integration of intelligent sensing devices, wearable systems, and networked medical equipment to facilitate advanced monitoring, diagnostics, and therapeutic interventions. This paper critically examines the technical challenges and recent technological advancements associated with the development of embedded systems tailored for IoMT applications. Major design constraints include real-time data acquisition and processing, low-power operation for prolonged device lifetime, hardware–software co-optimization, interoperability across heterogeneous platforms, and scalable network integration. Recent progress in miniaturized biomedical sensors, low-power wireless communication protocols (such as BLE, Zigbee, and LPWAN), and edge computing architectures has significantly enhanced system responsiveness, reliability, and distributed intelligence. These innovations enable continuous remote patient monitoring, data-driven personalized treatment strategies, and improved clinical decision support systems. Despite these advancements, security and privacy remain critical concerns due to the sensitive nature of medical data and the expanded attack surface of interconnected devices. Robust cryptographic frameworks, secure boot mechanisms, hardware-level authentication, intrusion detection systems, and strict compliance with healthcare regulatory standards are essential to ensure data integrity, confidentiality, and system resilience. This review synthesizes current literature, identifies existing research gaps, and highlights emerging trends aimed at developing secure, energy-efficient, interoperable, and scalable embedded architectures within the evolving IoMT ecosystem.

Keywords: Internet of Medical Things (IoMT), Embedded system design, Healthcare technology, Security and privacy

I. Introduction

In recent years, the intersection of healthcare and technology has given rise to the Internet of Medical Things (IoMT), a transformative field revolutionizing healthcare delivery through connected smart devices and sensors. IoMT covers a wide range of applications, from remote patient monitoring and real-time health data collection to personalized medicine and efficient medical device management [1]. This change promises to significantly improve patient care, treatment outcomes, and operational efficiency in healthcare facilities. The components of a remote patient monitoring system based on an IoT cloud architecture are shown in Figure 1 [2].

Embedded systems play a critical role in the IoMT by integrating advanced computing capabilities into medical devices and infrastructures (Figure 2). These systems enable seamless communication, data processing, and decision-making at the point of care, which is essential for supporting medical applications [3]. They are designed to operate efficiently within strict performance limits, process diverse sensor inputs, and ensure real-time response, which is critical for delivering reliable healthcare services.

However, the rapid proliferation of IoMT devices presents challenges, particularly with regard to the interoperability of different devices and platforms within IoMT networks. Seamless integration and communication between different vendors and protocols remains a significant obstacle, impacting the scalability and efficiency of IoMT deployments. Furthermore, it is important to ensure the security and confidentiality of sensitive medical data transmitted and stored by IoMT devices. The interconnectedness of IoMT networks increases vulnerability to cybersecurity threats and requires strong encryption, authentication mechanisms, and compliance with strict regulatory standards.

Innovations in sensor technology and wireless communication protocols have played a key role in enhancing IoMT capabilities. The increased accuracy and reliability of miniaturized sensors enable continuous monitoring of vital signs and chronic conditions, facilitating early detection of health problems and rapid intervention [4]. Furthermore, advances in edge computing enable IoMT devices to process data locally, reducing latency and bandwidth requirements while preserving

Current Journal of Engineering and Science Research
Volume 2, Issue 8, pp 24-28, August 2025
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2025.208005
Available Online at https://www.cjesr.com

patient privacy by minimizing data transfer to central servers. The integration of IoMT into clinical practice promises to revolutionize healthcare delivery models.

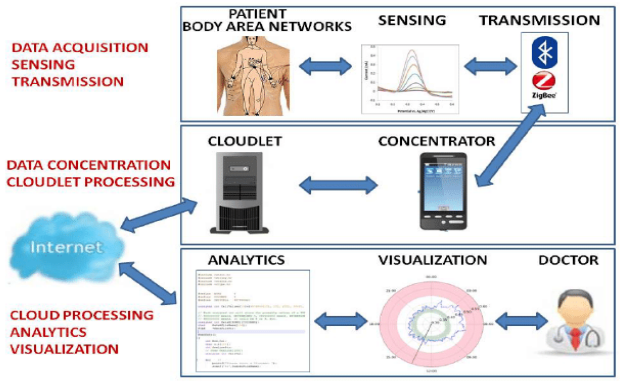

Figure 1: Elements of a remote patient monitoring system utilizing an IoT-Cloud architecture

Remote patient monitoring systems equipped with IoMT technologies allow healthcare professionals to monitor patients' health status remotely and in real time, enabling proactive interventions and personalized treatment plans. Furthermore, IoMT facilitates the aggregation of large amounts of patient-generated health data (PGHD), providing valuable insights into population health trends, disease management strategies, and healthcare resource optimization.

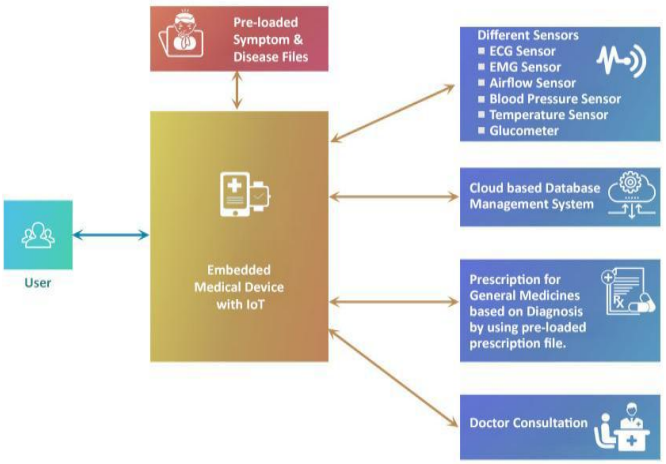

Figure 2: Embedded Systems in Medical Devices

Despite its transformative potential, IoMT faces challenges and obstacles. Regulatory complexities related to data protection, security standards, and medical device certifications vary across jurisdictions, posing compliance challenges for IoMT developers and healthcare organizations [5]. Furthermore, integrating IoMT into existing healthcare infrastructure requires significant investments in infrastructure, training, and support services to ensure seamless adoption and integration into clinical workflows.

In summary, the Internet of Medical Things (IoMT) represents a paradigm shift in healthcare and offers significant opportunities to improve patient outcomes, optimize operational efficiency, and transform medical practice. This article examines the challenges and innovations in integrated system design within IoMT applications and highlights key considerations for healthcare stakeholders, technology development, and regulatory stakeholders.

II. Challenges of Embedded System Design for the Internet of Medical Things (IoMT)

The development of embedded systems for the Internet of Medical Things (IoMT) presents several complex challenges that must be effectively addressed to ensure the reliability, efficiency, and security of healthcare applications. A major challenge is meeting the demanding requirements for real-time data processing and ensuring fast response times in the healthcare environment [6]. IoMT devices must process data quickly and accurately and operate within strict performance limits to extend battery life and minimize maintenance requirements.

Another critical challenge is achieving interoperability between different IoMT devices. These systems typically include devices from different manufacturers that use different communication protocols and standards. Seamless interoperability is critical for data exchange and the coordinated delivery of healthcare services. Standardization efforts are underway, but these are complicated by rapid technological advances and the diverse needs of healthcare facilities.

Security and privacy concerns are paramount for embedded IoMT systems. Given the sensitive nature of patient data processed by medical devices, these are often the target of cyberthreats. Ensuring robust cybersecurity measures such as data encryption, secure authentication methods, and compliance with regulatory standards such as HIPAA are critical. The interconnectedness of IoMT networks introduces additional complexity and requires continuous monitoring and proactive measures to protect patient data and device integrity.

Scalability and resource management present additional challenges in the development of integrated IoMT systems. As IoMT deployments continue to expand to serve larger patient populations and more complex healthcare environments,

Current Journal of Engineering and Science Research
Volume 2, Issue 8, pp 24-28, August 2025
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2025.208005
Available Online at https://www.cjesr.com

effectively managing resources such as bandwidth, storage, and computing power becomes increasingly difficult. Efficient resource allocation and optimization are essential to maintain system performance and reliability without compromising patient care or operational efficiency. Furthermore, the lifecycle management of integrated IoMT systems presents logistical hurdles. In addition, ongoing maintenance and updates are required to address vulnerabilities, improve functionality, and comply with constantly changing healthcare standards and regulations.

III. Innovations and Advances in Internet of Medical Things (IoMT) Devices

Significant advances in device technology have been made in the Internet of Medical Things (IoMT) space, fundamentally transforming healthcare and patient management. IoMT devices encompass a wide range of smart sensors, wearable devices, and medical devices connected via wireless networks, providing advanced capabilities for monitoring, diagnosing, and treating medical conditions [7].

A significant advancement in IoMT devices has been the evolution of sensor technologies. These advances have led to smaller, more accurate sensors capable of continuously and non-invasively monitoring vital signs such as heart rate, blood pressure, and blood glucose. Real-time data from these sensors enables early detection of health problems, facilitates timely interventions, and improves patient outcomes while reducing healthcare costs.

Improvements in wireless communication protocols have also played a critical role. Technologies such as Bluetooth Low Energy (BLE), Zigbee, and Wi-Fi Direct ensure reliable and secure connectivity between IoMT devices and central healthcare systems. This connectivity enables healthcare professionals to remotely monitor patient health, adjust treatment plans in real time, and ensure continuous care regardless of location.

Edge computing has become another key innovation in IoMT. By processing data locally on devices or at the network edge, edge computing reduces latency, minimizes bandwidth requirements, and improves data privacy. This approach is particularly advantageous for applications that require immediate responses, such as real-time monitoring and emergency medical care. It also supports advanced analytics and machine learning capabilities, enabling IoMT devices to analyze data patterns and provide personalized health recommendations based on individual patient profiles.

Furthermore, the integration of artificial intelligence (AI) and machine learning (ML) into IoMT devices has revolutionized diagnostic capabilities and treatment strategies. AI-powered IoMT systems can analyze large amounts of patient data, recognize patterns, and predict health outcomes with high accuracy. This capability facilitates personalized healthcare approaches, where treatment plans are tailored to a patient's individual needs based on comprehensive data analytics.

IV. Security and Privacy Concerns in IoMT

With the increasing adoption of the Internet of Medical Things (IoMT), significant concerns arise regarding the security and confidentiality of sensitive patient data and the reliability of medical devices. IoMT encompasses various interconnected devices, such as wearable sensors, implanted medical instruments, and remote monitoring systems, all of which rely on wireless networks [8]. This connection creates vulnerabilities that could be exploited by malicious actors.

One of the primary concerns of IoMT is the protection of patient data. These devices capture and transmit sensitive medical information such as medical history, diagnoses, and physiological data. To prevent unauthorized access and data misuse, strong encryption during data transmission and storage is essential. Compliance with healthcare regulations such as HIPAA in the US is crucial to maintaining the confidentiality of patient data and avoiding legal issues.

Cybersecurity threats pose significant risks to IoMT ecosystems. Medical devices are attractive targets for hackers seeking to disrupt healthcare services, steal patient information, or tamper with treatment processes. Vulnerabilities in device software, firmware, or network protocols can be exploited to gain unauthorized access to or control IoMT devices. Therefore, implementing strong authentication methods, regularly updating software, and conducting thorough security assessments are essential to mitigate these risks.

The challenge of interoperability between IoMT devices further complicates security initiatives. Devices from different manufacturers can differ in their security features and communication protocols, making it difficult to ensure consistent protection across IoMT networks. Standardizing security protocols and fostering collaboration between device manufacturers, healthcare professionals, and cybersecurity

Current Journal of Engineering and Science Research
Volume 2, Issue 8, pp 24-28, August 2025
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2025.208005
Available Online at https://www.cjesr.com

experts are essential steps toward addressing these interoperability issues.

Furthermore, continuous monitoring of IoMT networks and devices is essential to quickly detect and respond to security incidents. Proactive measures such as intrusion detection systems and real-time threat monitoring can help healthcare organizations minimize potential risks and maintain patient trust and safety in IoMT technologies. Regulatory and Ethical Considerations

The integration of Internet of Medical Things (IoMT) devices into healthcare requires careful attention to legal standards and ethical principles to ensure patient safety, data protection, and compliance with healthcare regulations. IoMT technologies such as wearable sensors, remote monitoring systems, and smart medical devices are subject to strict legal requirements and ethical guidelines due to their impact on patient care and healthcare operations [9]. Regulatory oversight is essential for the development, deployment, and use of IoMT devices. Laws such as the FDA regulations in the US and the Medical Device Regulation (MDR) in the European Union establish criteria for the safety, effectiveness, and quality of devices. Compliance with these regulations ensures that IoMT devices undergo rigorous testing, certification, and approval processes before being deployed in clinical settings. Furthermore, frameworks such as HIPAA require safeguards for patient health data and require IoMT developers and healthcare professionals to implement robust data protection measures and protocols. Ethical considerations in IoMT encompass several topics, including patient autonomy, informed consent, and equal access to healthcare services. Because IoMT devices collect and transmit sensitive patient data, preserving patient autonomy requires obtaining informed consent for data collection, use, and sharing. Transparent communication about the benefits, risks, and impacts of IoMT technologies is critical to enabling patients to make informed decisions about their healthcare. Furthermore, ensuring equal access to IoMT technologies is essential to avoiding healthcare disparities. Ethical guidelines advocate for equitable distribution and affordability of IoMT devices and ensure that all patient populations, including underserved communities, can benefit from technological advances in healthcare.

V. Future Directions and Conclusion

The Internet of Medical Things (IoMT) promises significant advances in the future that could revolutionize healthcare and patient care. One key direction for IoMT is the integration of artificial intelligence (AI) and machine learning (ML) algorithms into medical devices. AI-powered IoMT systems have the potential to analyze comprehensive patient data in real time, enabling predictive analytics for early disease detection, personalized treatment recommendations, and automated healthcare decision-making. These advances could transform diagnosis, improve treatment outcomes, and optimize healthcare resource allocation. Furthermore, continued advances in sensor technology and wearable devices are expected to improve the accuracy, reliability, and usability of IoMT systems. Smaller sensors that can continuously monitor various health parameters enable more accurate health monitoring. Integrating wearable devices with IoMT technologies enables patients to actively participate in managing their healthcare, promoting preventative care and early intervention strategies. In summary, while IoMT offers significant opportunities to improve healthcare efficiency and patient outcomes, several challenges must be addressed to fully realize its benefits. These challenges include ensuring compatibility between different devices, strengthening cybersecurity measures to protect patient data, and adapting to regulatory frameworks to ensure patient adherence and safety. By addressing these challenges and embracing future advances in AI, sensors, and wearable technologies, IoMT is poised to revolutionize healthcare, making it more personalized, accessible, and efficient for patients worldwide.

REFERENCES

[1] Joyia, Gulraiz J., et al. "Internet of medical things (IoMT): Applications, benefits and future challenges in healthcare domain." J. Commun. 12.4 (2017): 240-247.

[2] Rahmani, Amir M., et al. "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach." Future Generation Computer Systems 78 (2018): 641-658.

[3] Jonnerby, Jakob, A. Brezger, And H. Wang. "Machine learning based novel architecture implementation for image processing mechanism." International Journal of communication and computer Technologies 11.1 (2023): 1-9.

[4] G. Sasikala, & G. Satya Krishna. (2023). Low Power Embedded SoC Design. Journal of VLSI Circuits and Systems, 6(1), 25–29. https://doi.org/10.31838/jvcs/06.01.04.

[5] Srivastava, Jyoti, et al. "[Retracted] Internet of Medical Things (IoMT)-Based Smart Healthcare System: Trends and Progress." Computational Intelligence and Neuroscience 2022.1 (2022): 7218113.

Current Journal of Engineering and Science Research
Volume 2, Issue 8, pp 24-28, August 2025
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2025.208005
Available Online at https://www.cjesr.com

[6] Hatzivasilis, George, et al. "Review of security and privacy for the Internet of Medical Things (IoMT)." 2019 15th international conference on distributed computing in sensor systems (DCOSS). IEEE, 2019.

[7] Cide, Felip, José Urebe, and Andrés Revera."Exploring Monopulse Feed Antennas for Low Earth Orbit Satellite Communication: Design, Advantages, and Applications." National Journal of Antennas and Propagation 4.2 (2022): 20-27.

[8] Razdan, Sahshanu, and Sachin Sharma. "Internet of medical things (IoMT): Overview, emerging technologies, and case studies." IETE technical review 39.4 (2022): 775-788.

[9] Vishnu, S., SR Jino Ramson, and R. Jegan. "Internet of medical things (IoMT)-An overview." 2020 5th international conference on devices, circuits and systems (ICDCS). IEEE, 2020.

[10] Zanella, Andrea, et al. "Internet of things for smart cities." IEEE Internet of Things journal 1.1 (2014): 22-32.

[11] Arandia, Nerea, Jose Ignacio Garate, and Jon Mabe. "Embedded sensor systems in medical devices: Requisites and challenges ahead." Sensors 22.24 (2022): 9917.

[12] Karam, Asaad Ali. "Investigating the importance of ethics and security on internet of medical things (IOMT)." International Journal of Computations, Information and Manufacturing (IJCIM) 2.2 (2022).

Citation of this Article:

Dewi Kartika, Fajar Hidayat, Arif Wijaya, & Siti Wulandari. (2025). Next-Generation Embedded Systems for IoMT: Design Constraints and Opportunities. *Current Journal of Engineering and Science Research*. 2(8), 24-28. Article DOI: https://doi.org/10.47001/CJESR/2025.208005

***** End of the Article *****