Journal of Engineering Science *Vol. XXXII, no. 4 (2025), pp. 29 - 40*
Fascicle *Electronics and Computer Science* *ISSN 2587-3474*
Topic *Biomedical Engineering* *eISSN 2587-3482*

https://doi.org/10.52326/jes.utm.2025.32(4).03
UDC 681.586:61:004.738.5

SENSING LAYER TECHNOLOGIES AND NETWORKING ON THE INTERNET OF MEDICAL THINGS

Victor Moraru *, ORCID: 0000-0002-5454-8341,
Dorin Gribincea, ORCID: 0009-0005-1505-9763,
Emilian Guțuleac, ORCID: 0000-0001-6839-514X

Technical University of Moldova, 168 Stefan cel Mare Blvd., Chisinau, Republic of Moldova
* Corresponding author: Victor Moraru, *victor.moraru@calc.utm.md*

Received: 12. 04. 2025
Accepted: 12. 27. 2025

Abstract. Internet of Medical Things (IoMT) apply engineering principles and design to medicine and biology to improve healthcare outcomes. This interdisciplinary field bridges engineering and medicine by integrating the innovative and analytical strengths of engineering with medical and biological expertise, resulting in more effective approaches to diagnosing, monitoring, and treating patients. This article focuses on exploring the key components and strategies of the sensing layer in the IoMT, including medical devices, smart sensors, biomedical sensors, wireless technologies, communication protocols, and the associated challenges of reliability and security. Several critical factors must be taken into account when designing IoMT sensing layer networks, such as body movement, temperature variation, energy efficiency, transmission range and heterogeneous environments.

Keywords: *Internet of Medical Things,* smart sensors*, biosensors, sensor layer protocols, wireless sensor body network.*

Rezumat. Internetul Lucrurilor Medicale (ILM) aplică principii inginerești de proiectare în medicină și biologie pentru a îmbunătăți rezultatele asistenței medicale. Acest domeniu interdisciplinar face legătura între inginerie și medicină prin integrarea punctelor forte inovatoare și analitice ale ingineriei cu expertiza medicală și biologică, rezultând abordări mai eficiente pentru diagnosticarea, monitorizarea și tratarea pacienților. Acest articol se concentrează pe explorarea componentelor și strategiilor cheie ale nivelului de detectare în ILM, inclusiv dispozitive medicale, senzori inteligenți, senzori biomedicali, tehnologii wireless, protocoale de comunicație și provocările asociate legate de fiabilitate și securitate. La proiectarea stratului de percepție al ILM trebuie luați în considerare mai mulți factori critici, cum ar fi mișcarea corpului, variația temperaturii, eficiența energetică, distanța de transmisie și mediile eterogene.

Cuvinte cheie: *Internetul Lucrurilor Medicale, senzori inteligenți, biosenzori, protocoale ale stratului de percepție, rețea corporală de senzori fără de fir*

1. Introduction

Biomedical systems apply engineering concepts and design principles to the fields of medicine and biology to improve healthcare outcomes. This discipline seeks to bridge the gap between engineering and medicine by merging the innovative and analytical capabilities of engineering with expertise in medical and biological sciences, resulting in more advanced techniques for diagnosis, monitoring, and treatment. These systems involve a wide range of applications, including medical imaging, prosthetics, implantable devices, and healthcare information systems. Additionally, the integration of biomedical systems with artificial intelligence represents a growing and dynamic area of research.

The advancement of biomedical systems typically requires a multidisciplinary collaboration, drawing on knowledge from medicine, engineering, and computer science. Progress in this field holds the promise of enhancing patient care and transforming the delivery of healthcare services.

One of the most effective and beneficial methods to put biomedical systems into practice is by using established and widely recognized approaches such as Wireless Sensor Networks. These networks gain additional significance when we take into account their connection with the Internet of Things (IoT) and their application in the healthcare domain [1]. This combination allows for greater connectivity and data exchange between medical devices and applications, leading to improved health monitoring and patient care. By harnessing these technologies, healthcare providers can collect and analyze patient data more efficiently, enabling timely interventions and better management of health conditions. Overall, making use of along with the IoT [2] represents a significant advancement in the implementation of biomedical systems, paving the way for innovative solutions in health care.

The Internet of Medical Things (IoMT) [3], a specific application of IoT in biomedicine, plays an important role in the advancement of biomedical systems and presents various advantages for the healthcare sector. By integrating the core technologies and functionalities of the IoT into healthcare, IoMT creates considerable opportunities to enhance patient care, streamline clinical processes, and support healthcare providers in making informed decisions based on data.

The IoMT defines a network of interconnected medical sensors, devices, applications, and services that utilize internet-enabled technologies to facilitate real-time health monitoring and management.

2. Sensing Layer as Element of IoMT Architecture

When creating solutions for the IoMT there are several critical elements that must be thoughtfully addressed to achieve a successful outcome. A primary consideration is the security of both the devices and the data they process since these products frequently gather sensitive information from patients. Another vital element is interoperability which pertains to the ability of various devices to communicate and collaborate effectively within a healthcare framework. Additionally, usability plays a key role because it is important for devices to be accessible for both medical practitioners and patients ensuring they can be used easily and efficiently.

In addition, it is crucial to assess the reliability and sturdiness of the devices as they must operate correctly in diverse healthcare settings and scenarios. This means ensuring they can endure regular use and any potential physical challenges they might encounter. Finally

adhering to regulatory standards is another important consideration since all medical devices are required to follow specific regulations and guidelines established by health organizations to guarantee safety and efficacy. In summary these elements are essential for the effective design and implementation of IoMT solutions within the healthcare sector.

Aspects to consider in the design of IoMT:

- *User mobility*. One challenge lies in maintaining communication strength when the network topology changes due to a user's movement, as sensor devices and medical equipment may move with the user. To tackle this unpredictable issue, the IoMT routing protocol should be adaptable, ensuring robust communication while not compromising quality.
- *Energy consumption optimization*. Energy efficiency plays a vital role in influencing the size, operational lifespan, and overall usability of a device. The used by IoMT routing protocol should, thus, focus on optimizing energy consumption to ensure adequate device performance. For implantable devices, a battery life of at least 10 to 15 years is necessary to avoid frequent surgeries and their associated costs. Wearable devices depend on frequent battery replacements to maintain usability.
- *Connectivity and transmission range*. Shorter transmission ranges may lead to disconnections and reorganization among sensor nodes in an IoMT system due to body movements.
- *Heterogeneous environment*. The IoMT routing protocol for Wireless Body Sensor Networks (WBSNs) should be capable of handling heterogeneous environments common in WBSN applications.
- *Quality of Service (QoS)*. In real-time applications, like ECG, data loss and delays can be detrimental. Consequently, QoS requirements should be addressed to ensure efficient handling of such scenarios, especially for implanted smart sensors with fixed memory and computational capabilities.
- *Interoperability and compatibility* are essential within the IoMT framework to enable seamless communication and data sharing among different healthcare devices and systems. The use of standardized communication protocols and health data exchange formats is key to achieving effective interaction between diverse IoMT components.
- *User interfaces and applications* serve as access points for healthcare professionals, caregivers, and patients to interact with the IoMT system. Tools like mobile applications, web platforms, and specialized medical software support real-time health monitoring, data visualization, and remote healthcare services.
- *Security and privacy* are ensured through robust measures including encryption, authentication, and access control, which protect sensitive patient information from unauthorized access. While cloud storage enables quick and accurate responses from IoMT devices, it also introduces potential risks such as data breaches or misuse.

The structure of the Internet of Medical Things consists of a complex and detailed architecture. This system is essential for connecting an array of medical devices, specific software solutions, and a variety of healthcare platforms. The main objective of this integration is to greatly enhance patient care while optimizing different healthcare processes. Through this technological and healthcare fusion, IoMT strives to facilitate smoother operations that are advantageous for both patients and healthcare professionals. Ultimately, this integrated network is designed to raise the quality of medical care and optimize the efficiency and effectiveness of healthcare delivery. In the simplest case there are four primary

elements in IoMT: medical devices and sensors, connectivity, data management and application, respectively four layers in the IoMT architecture: sensing, networking, cloud infrastructure and application and decision-making layers as shown in Figure 1.

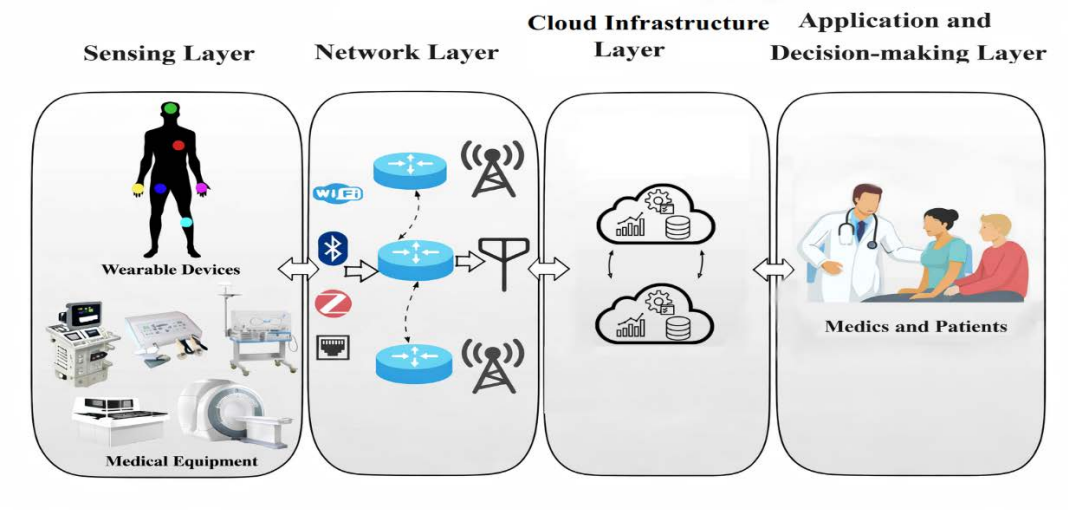

Figure 1. Four layers IoMT architecture.

The sensing layer, also referred to as the perception layer, forms the foundation of the IoMT architecture and plays a crucial role in collecting and organizing data from various physical devices. Its importance is particularly evident in IoMT systems, as it directly interacts with medical sensors and equipment. In this context, the sensing layer captures information from devices like heart rate monitors, glucose meters, and various wearable or implantable technologies. It acts as a critical bridge between the physical medical environment and the digital domain where data is processed and analyzed.

Sensors are instruments that detect physical, chemical, or biological signals and enable the measurement and recording of those signals. For instance, tactile sensors, often made from piezoelectric materials, produce voltage in response to touch, pressure, bending or temperature changes.

Actuators, on the other hand, perform specific actions based on data received from sensors or user interaction. An example is an actuator with an integrated reservoir and pump that delivers the appropriate dose of insulin to a diabetic patient according to glucose level readings.

3. Medical Sensors and Devices

The IoMT sensing layer operates with various devices and different kinds of sensors, which can be classified as wearable devices and medical equipment

Wearable devices are made to be worn or attached to the body to track health and provide important medical data. Depending on their use, these devices can be divided into consumer wearables, clinical wearables, implantable devices, and ambient devices.

Consumer wearables are mainly used for tracking body signals in real-time, like blood pressure and heart activity, as well as behaviors such as movement and speed.

An implantable device is a medical instrument inserted into a patient's body through surgery. Notable examples of advanced implantable technology include pacemakers and digital pills, also referred to as smart pills. Modern ingestible devices, such as capsule

endoscopes, are capable of gathering gastrointestinal data over extended periods outside clinical settings, with the potential for additional sensors to enhance data collection.

Ambient devices include a range of environmental sensors such as motion detectors, contact switches, beam-break sensors, and pressure mats used to monitor environmental conditions or detect changes in locations like homes and workplaces.

Medical equipment refers to tools for medical imaging, biochemistry analysis, and bedside monitoring used to detect diseases in hospitals.

Medical imaging equipment consists of diagnostic tools that provide information about the body's structure using techniques such as MRI, CT scans, and ultrasounds. The images produced are usually large and don't need to be processed in real-time.

The biochemistry analyzer is used to identify different biochemical markers in the body, and it produces smaller amounts of data with less need for immediate processing.

The bedside monitor is used to continuously watch a patient's body readings in hospital rooms, relying on real-time data to quickly alert staff to any urgent situations.

One of the most important groups of sensors that we can find in various applications is known as biosensors. These devices are specially designed to detect and measure biological changes or substances in a given environment (see the Figure 2). A biosensor is a device designed to detect biological or chemical reactions by producing signals that correspond to the concentration of a specific analyte involved in the reaction [5]. These sensors are used in various applications, including disease tracking, pharmaceutical research, and the identification of environmental pollutants, harmful microorganisms, or disease-related markers present in bodily fluids such as blood, urine, saliva and sweat.

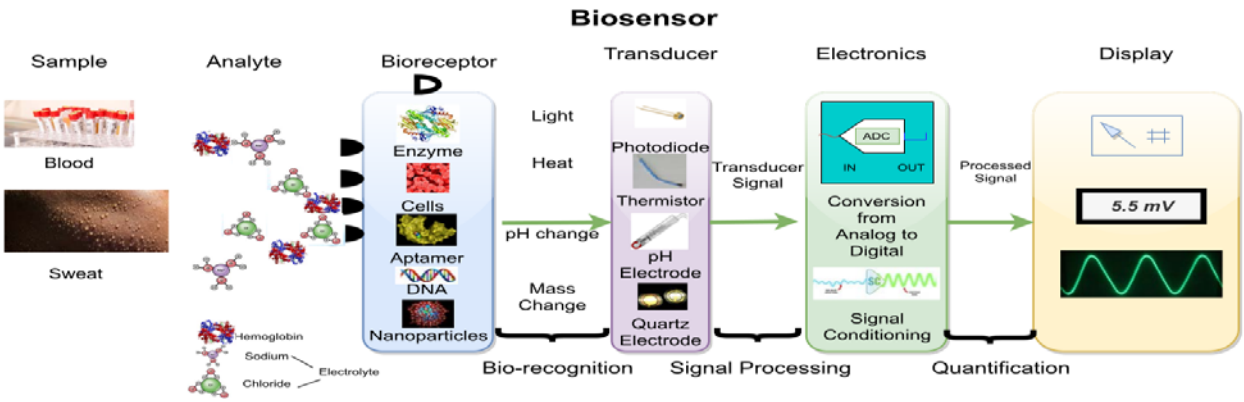

Figure 2. Schematic representation of a biosensor [6].

All body sensors [7,8] are integrated into a wireless body sensor network, which can be defined as a specialized form of mobile personal area network. This network allows multiple sensors, strategically embedded or worn on the body, to communicate without the need for wires or cables. The wireless aspect of this network enables the sensors to transmit vital health data in real-time, facilitating continuous monitoring of physiological parameters. By creating this interconnected system, it becomes possible for the sensors to work collaboratively, providing comprehensive insights into an individual's health status while also enhancing the overall effectiveness of medical interventions

Each body sensor needs to connect wirelessly to a specific device that is referred as mobile multiprotocol Personal Access Point (PAP) as shown in Figure 3. This important device is responsible for collecting all the information from these sensors. Once it gathers the data,

PAP transmits this information to the next level of the IoMT system, ensuring that the collected data are effectively shared and utilized in a connected healthcare network.

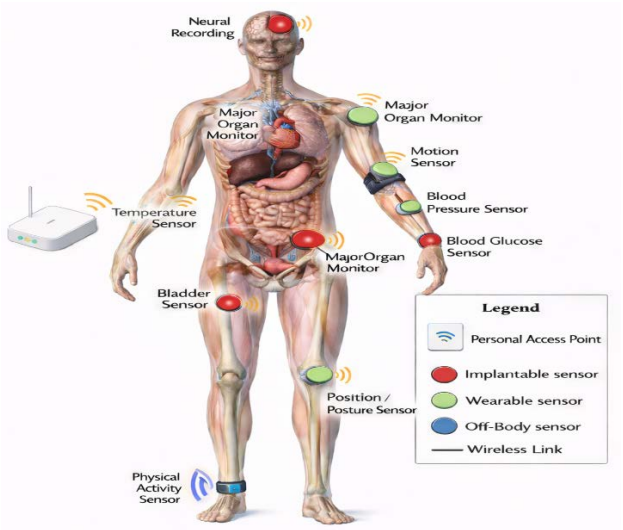

Figure 3. Wearable wireless body sensor network.

4. IoMT Sensing Layer Networking and Communications

The sensor layer is the essential component of the IoMT system, tasked with collecting data from patients using various sensors and transmitting this information to the network layer for further transmission and processing. It includes hardware components like sensors, controllers, and actuators, which allow for accurate detection of health-related parameters.

The sensor layer consists of two main sublayers: data-processing and data-entry. The primary role of the data-processing sublayer is to analyze the incoming data by employing various signal acquisition and medical perception technologies. The collected data are then sent to the next stage through the data-entry sublayer, which uses short-range and lower power transmission methods. The main technologies and protocols used on this layer are described below.

Infrared Data Association (IrDA). Infrared technology developed by the Infrared Data Association (IrDA) [10] enables short-range communication between devices using infrared light. IrDA establishes standards for wireless infrared communication that operates over a few meters through focused infrared beams. The IrDA protocol consists of three key layers: the physical layer, the link access protocol (IrLAP), and the link management protocol (IrLMP). IrLAP is responsible for establishing a basic connection between two devices, using the High-level Data Link Control standard to manage connections and data transmission. IrLMP allows different components within IrDA devices to communicate simultaneously through a single IrLAP connection and supports service discovery between devices. The device discovery process identifies the address of nearby devices, their IrLAP version, and additional discovery data defined by the IrLMP layer. In the healthcare field, IrDA technology is applied in devices such as thermometers and infrared cameras, particularly in temperature sensors. Additionally, infrared thermal imaging is used to capture body images and measure surface temperature.

Radio Frequency Identification (RFID) [11] is a wireless technology that helps identify things using radio signals for short-distance communication. The two main parts of RFID are the RFID reader and the RF tag, which is the device that responds to the signals. The RFID reader can store data and read information from a distance. When the RF tag gets a signal from the reader, it replies with identification details and other information. This identification

usually includes a unique serial number, and the extra information might include product details like stock numbers and production dates. There are two main types of RFID tags: active tags and passive tags. Active tags have their own power source and work on higher frequency bands, making them more expensive. Passive tags, on the other hand, operate at lower frequencies and do not have a power supply inside. The common frequency ranges for RF communications are: (a) Low Frequency (LF) at 125 kHz, (b) High Frequency (HF) at 13.56 MHz, (c) Ultra High Frequency (UHF) from 433 MHz to 860–960 MHz, and (d) Microwave frequencies at 2.45 GHz and 5.8 GHz. RFID tags that are placed inside or near a patient's body are important for creating healthcare systems that do not bother the patient. Passive RFID tags can also be used to monitor the patient's surroundings, helping to spot changes in physical or chemical conditions. RFID technology is also used for controlling access; for example, hospitals might use RFID cards to secure entry. Another use of RFID involves tags and sensors that monitor temperature closely for storing medications, ensuring the right temperature is maintained for different drugs.

Near Field Communication (NFC) [12] is a way for devices to communicate over very short distances, usually just a few centimeters. NFC is set by standards called ECMA-340 and ISO/IEC 18092. It works by using magnetic fields to connect the sending and receiving devices and operates at a frequency of 13.56 MHz, allowing data to transfer at speeds up to 424 Kbps. Like RFID, NFC can work in both active and passive ways. In passive mode, one device creates a radio field, which powers the other device using the energy from the first device. NFC makes it easy and cheap to connect Internet of Things (IoT) devices.

Bluetooth/BLE is a popular wireless technology that follows the IEEE 802.15.1 standard. It is made for devices that use little power and are affordable, working in the 2.4 GHz frequency range. Bluetooth allows for Personal Area Networks (PAN) in a star layout, which means it uses less power, sets up quickly, and can connect many devices easily. It is great for short-distance data transfer between mobile devices. The range can vary by version; for example, version 2.1 can go up to 100 meters indoors, while version 5 (BLE) can reach up to 400 meters. Different Bluetooth versions can send data at speeds of up to 2 Mbps. The low-power version is called Bluetooth Low Energy (BLE) [13] or Bluetooth Smart. The latest version, BLE 5.0, also has a data speed of 2 Mbps and uses less power because it transmits data faster. This shorter transmission time helps devices work better together. When compared to other low-power wireless technologies like ZigBee or Z-Wave, BLE has the highest data speeds, even at its original rate of 1 Mbps. Bluetooth does need devices to pair, but it uses more power than NFC.

Bluetooth Low Energy (BLE) is commonly used in IoT networks involving battery-operated, energy-efficient, and cost-effective devices. It enables fast connectivity and supports straightforward device-to-device communication or star network configurations. BLE is particularly well-suited for IoMT applications that require short-range communication, rapid response times, and minimal data transmission. This makes it ideal for Human Interface Devices (HIDs), fitness trackers and portable medical equipment.

Z-Wave [14] is a smart home communication protocol that uses various techniques to keep your information safe and secure. It incorporates encryption, which is a method of scrambling data to protect it from unauthorized access. In addition to encryption, Z-Wave also employs behavior detection, which helps to identify and respond to unusual activities that might indicate a security threat. Another important feature is proximity security, which

adds an additional layer of protection by ensuring that devices communicate only when they are physically close to each other.

The protocol has a specific mechanism called the "Security" command class, which plays a crucial role in safeguarding the data. This mechanism is designed to maintain the confidentiality of information, which means that only authorized users can access the data. It also ensures source integrity, meaning that the information comes from a legitimate source, and data integrity, which guarantees that the information has not been altered or compromised in any way.

To achieve these security goals, Z-Wave uses special techniques for securing both the payloads, which are the actual data being sent, and the frames, which are the structures that carry the data. The data is protected through a powerful method called AES encryption, which stands for Advanced Encryption Standard. This encryption method is widely recognized for its effectiveness in keeping information secure. Z-Wave utilizes three shared keys to help manage encryption and decryption processes, ensuring a robust defense against unauthorized access and maintaining a high level of security for all communications within its network.

The Ultra-Wideband (UWB) protocol [15], based on the IEEE 802.15.3 standard, is specifically designed to support high-speed, short-range indoor wireless communication. Capable of delivering data rates between 110 and 480 Mbps, UWB is ideal for bandwidth-intensive applications such as audio and video streaming in home networks. Due to its wide bandwidth, UWB can act as a wireless alternative to high-speed cable connections like USB 2.0 and IEEE 1394. Regulatory frameworks for UWB vary worldwide. In the U.S., the Federal Communications Commission allocated spectrum for UWB in February 2002, while the European Commission established regulatory guidelines in February 2007 for all EU member states. UWB operates differently from conventional wireless technologies. Instead of modifying the power, frequency, or phase of a continuous wave, it transmits information by emitting radio pulses at specific time intervals across a broad frequency range, using techniques such as pulse-position modulation. Its low power consumption and precise signal timing make UWB well-suited for real-time applications in environments sensitive to radio frequency interference, such as hospitals

ZigBee [16] is a wireless communication protocol that adheres to the IEEE 802.15.4 standard. It is known for being low-cost, low-power, and low-speed, with a communication range of up to 100 meters and data rates ranging from 40 to 250 Kbps. Operating at 915 MHz and 2.4 GHz, ZigBee is intended for Personal Area Networks (PANs) and supports multiple network topologies, including star, tree, and mesh configurations, accommodating up to 65,000 nodes per network.

Widely used in IoT applications, ZigBee is particularly valuable in healthcare for connecting sensors to central coordinators and facilitating communication between multiple coordinators. In 2009, the ZigBee Alliance introduced the ZigBee Health Care public application profile, which was developed for assistive, non-invasive healthcare devices. Based on ZigBee Pro, this profile offers a standardized application layer protocol tailored for healthcare settings, ensuring interoperability among various medical and non-medical devices.

A summary of the current communication protocols and technologies used in the IoMT sensing layer is presented in Table 1.

Table 1

IoMT Sensing Layer Communication Protocols and Technologies [10-17]

Protocol/Technology	Frequency	Data Rate	Range	Power consumption
IrDA	850–900 nm	14.4 Kbps	1 m	Not available
RFID	13.56 MHz	106 – 424 Kbps	20 cm	Very low
NFC	13.56 MHz	106 – 424 Kbps	20 cm	Very low
Bluetooth/BLE	2.4 GHz	1, 2, 3 Mbps	80 – 90 m	Low
ZWave	800–900 MHz	40 Kbps	30 m	Low
UWB	3.1–10.6 GHz	53 – 480 Mbps	10 m	Very low
ZigBee	2.4 GHz	250 Kbps	100 m	Low

5. Recent Related Work on Technologies and Networking in the IoMT Sensing Layer

Recent research on the Internet of Medical Things (IoMT) has increasingly focused on the *networking aspects of the sensing (perception) layer*, which serves as the primary interface between physiological data acquisition and higher-level processing layers. This layer is composed of wearable, implantable, and ambient sensors that collect biomedical signals and transmit them to local gateways or coordinators under strict constraints related to energy consumption, latency, reliability, and security.

A predominant architectural model discussed in recent literature (2023–present) is the WBAN, which enables short-range communication among heterogeneous medical sensors deployed on or inside the human body. WBAN-based architectures are widely regarded as the most suitable networking paradigm for the IoMT sensing layer due to their support for low-power operation and patient mobility. Zhou *et al*. [18] provide a comprehensive survey of wireless communication solutions for IoMT, identifying WBANs as the cornerstone of sensing-layer connectivity in modern medical monitoring systems.

With respect to communication technologies, recent studies highlight the dominance of *short-range wireless protocols* at the sensing layer. *Bluetooth Low Energy* is consistently reported as the most prevalent technology, owing to its low energy consumption, adequate throughput for physiological data, and native support in consumer devices such as smartphones and smartwatches. BLE is particularly suitable for continuous health monitoring applications requiring long device lifetimes. In parallel, *ZigBee and IEEE 802.15.4-based protocols* remain relevant in multi-sensor scenarios, where mesh networking and scalability are required [19]. Additionally, *Ultra-Wideband* has gained attention for its high localization accuracy and robustness against interference, although its practical deployment in IoMT sensing systems remains limited due to higher complexity and power requirements.

Recent works also emphasize the increasing use of *hybrid and multi-tier communication architectures*. In these architectures, short-range wireless technologies are employed for intra-WBAN communication, while data forwarding to remote servers is handled by Wi-Fi or cellular-enabled gateways. He notes that such hybrid approaches improve scalability and quality of service while preserving energy efficiency at the sensor level [19]. This layered communication strategy reflects the growing heterogeneity of IoMT systems and the need for flexible networking solutions.

A notable trend in post-2023 literature is the integration of *local data pre-processing and edge intelligence* within sensing devices. Instead of transmitting raw biomedical signals, sensors increasingly perform signal conditioning, feature extraction, or event detection prior to communication. This approach significantly reduces network traffic and latency while extending sensor battery life, which is critical for long-term and dense sensing deployments. Zhou *et al*. [18] identify communication-aware sensing and edge-assisted data reduction as key enablers for scalable IoMT networks.

Security and interoperability remain critical challenges at the sensing layer. Recent studies indicate that conventional IoT security mechanisms are often inadequate for medical applications due to the sensitivity of health data and the life-critical nature of IoMT services. Consequently, current research focuses on lightweight encryption, authentication, and key management schemes tailored to resource-constrained sensing devices. Jayousi [20] further emphasizes that the lack of standardization across communication protocols hinders interoperability and large-scale deployment of IoMT systems, motivating ongoing efforts toward unified communication frameworks.

Emerging research directions also consider the indirect impact of *5G-enabled gateways and future 6G communication paradigms* on sensing-layer networking. While cellular technologies are not directly employed by sensing nodes, their support for ultra-reliable low-latency communication influences system-level design requirements and gateway–sensor interaction models, particularly for real-time and remote healthcare applications.

In summary, recent related work characterizes the IoMT sensing layer as a resource-constrained yet highly dynamic networking environment. Current trends emphasize WBAN-centric architectures, energy-efficient short-range wireless technologies, intelligent data reduction at the source, and enhanced security and interoperability mechanisms. These developments aim to support reliable, scalable, and patient-centric IoMT systems capable of meeting the stringent demands of next-generation digital healthcare.

6. Conclusions

The IoMT sensing layer allows healthcare professionals to make informed decisions using real-time data from physical devices, which is crucial for better patient care and health monitoring. It serves as a vital connection between the physical world of medical devices and sensors and the digital realm where data is processed and analyzed. By enabling continuous and non-invasive monitoring, the sensing layer contributes to early diagnosis, timely intervention, and personalized treatment plans.

The IoMT sensor layer's emerging communication technologies must utilize short-range and low-power approaches to minimize inter-body interference and reduce battery consumption. Protocols such as BLE, Zigbee, and NFC are being increasingly adopted due to their efficiency in maintaining reliable connectivity while preserving energy. These technologies ensure the seamless transmission of patient data from wearable or implantable devices to local hubs or gateways for further analysis.

As the sensor layer continues to evolve, emphasis must also be placed on ensuring data security and patient privacy. Implementing robust encryption protocols and authentication mechanisms is essential to prevent unauthorized access to sensitive health information. Together, these technological and structural enhancements reinforce the IoMT sensing layer as a foundational component of modern, intelligent healthcare ecosystems.

This research was conducted within the LifeTech project at the Technical University of Moldova, the results were presented in the Biomedical Section of the 13th International Conference on Electronics, Communications, and Computing (IC ECCO-2024), organized by the Technical University of Moldova, held in Chișinău, Moldova, on October 17–18, 2024.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Dang, L.M.; Piran, M.J.; Han, D.; Min, K.; Moon, H. A Survey on Internet of Things and Cloud Computing for Healthcare. *Electronics* 2019, 8, 768. https://doi.org/10.3390/electronics8070768
2. Banka, S., Madan, I., Saranya S. S. Smart healthcare monitoring using IoT. *International Journal of Applied Engineering Research* 2018, 13(15), 11984.
3. Vishnu, S. Ramson, S.R.J.; Jegan, R. Internet of Medical Things (IoMT) - An overview. In: *5th International Conference on Devices, Circuits and Systems (ICDCS)*, Coimbatore, India, 2020, pp. 101-104, https://doi.org/10.1109/ICDCS48716.2020.243558.
4. Li, N.; Xu, M.; Li, Q.; Liu, J.; Bao, S.; Li, Y.; Li, J.; Zheng, H. A review of security issues and solutions for precision health in Internet-of-Medical-Things systems. *Security and Safety* 2023, 2, 2022010, https://doi.org/10.1051/sands/2022010.
5. Bhalla, N; Jolly P; Formisano, N; Estrela, P. Introduction to biosensors. *Essays Biochem* 2016, 60 (1), pp. 1–8. doi: https://doi.org/10.1042/EBC20150001.
6. Zhou, Y.; Fang, Y.; Ramasamy, R. Non-covalent functionalization of carbon nanotubes for electrochemical biosensor development. *Sensors* 2019, 19(2), 392.
7. Global Biomedical Sensors Market 2020, Application, Analysis. Available online: URL https://www.openpr.com/news/2135530/global-biomedical-sensors-market-2020-application-analysis (accessed on 16 October 2024)
8. Shen, G. Recent advances of flexible sensors for biomedical applications. Progress in Natural Science, *Materials International* 2021, 31(6), pp. 872-882.
9. Seçkin, M.; Seçkin, A. Ç.; Gençer, Ç. Biomedical sensors and applications of wearable technologies on arm and hand. *Biomedical Materials & Devices* 2023, 1, pp. 443-455.
10. Megowan, P.J.; Suvak, D. W.; Knutson, C. D. IrDA infrared communications: An overview. *Counterpoint Systems Foundry* 1996, 96.
11. Landaluce, H.; Arjona, L.; Perallos, A.; Falcone, F.; Angulo, I.; Muralter, F. A Review of IoT Sensing Applications and Challenges Using RFID and Wireless Sensor Networks. *Sensors* 2020, 20, 2495. https://doi.org/10.3390/s20092495
12. Liu, Y.; Wang, Z.; Xu, J.; Ouyang, C.; Mu, X.; Schober, R. Near-field communications: A tutorial review. *IEEE Open Journal of the Communications Society* 2023, 4, pp. 1999-2049.
13. Zhang, T.; Lu, J.; Hu, F.; Hao, Q. Bluetooth low energy for wearable sensor-based healthcare systems. In: *IEEE Healthcare Innovation Conference (HIC)*, Seattle, WA, USA, 2014, pp. 251-254, https://doi.org/10.1109/HIC.2014.7038922.
14. Molisch, A. F. Ultra-wideband communications: An overview. *URSI Radio Science Bulletin* 2009, 329, pp. 31-42.
15. Dhillon, P.; Sadawarti, H. A review paper on zigbee (IEEE 802.15.4) standard. *International journal of engineering research and technology* 2014, 3(4), pp. 141-145.
16. Buthelezi, B.E.; Mphahlele, M.; DuPlessis, D.; Maswikaneng, S.; Mathonsi, T. ZigBee healthcare monitoring system for ambient assisted living environments. *International Journal of Communication Networks and Information Security* 2019, 11(1), pp. 85-92.
17. Askar, N. A.; Habbal, A.; Mohammed, A. H.; Sajat, M. S.; Yusupov, Z.; Kodirov, D. Architecture, protocols, and applications of the internet of medical things (IoMT). *Journal of Communications* 2022, 17(11), pp. 900-918.
18. Zhou, J.; Sun, Y.; Tellambura, C. Revolutionizing medical data transmission with the Internet of Medical Things: A comprehensive survey of wireless communication solutions and future directions. *arXiv preprint arXiv* 2504.02446, https://doi.org/10.48550/arXiv.2504.02446
19. He, P.; Huang, D.; Wu, D.; He, H.; Wei, Y.; Cui, Y.; Peng, L. A survey of internet of medical things: technology, application and future directions. *Digital Communications and Networks* 2024, https://doi.org/10.1016/j.dcan.2024.11.013.

20. Jayousi, S.; Barchielli, C.; Guarducci, S.; Alaimo, M.; Caputo, S.; Zoppi, P.; Mucchi, L. From innovation to integration: bridging the gap between IoMT technologies and real-world health management systems. *Sensors* 2025, *25*(21), 6660.

Citation: Moraru, V.; Gribincea, D.; Guțuleac, E. Sensing layer technologies and networking on the internet of medical things. *Journal of Engineering Science*. 2025, XXXII (4), pp. 29-40. https://doi.org/10.52326/jes.utm.2025.32(4).03.

Submission of manuscripts: jes@meridian.utm.md