applied sciences

MDPI

Article

Framework for a Secure and Sustainable Internet of Medical Things, Requirements, Design Challenges, and Future Trends

William Villegas-Ch [1,*], Joselin García-Ortiz [1] and Isabel Urbina-Camacho [2]

[1] Escuela de Ingeniería en Ciberseguridad, FICA, Universidad de Las Américas, Quito 170125, Ecuador; joselin.garcia.ortiz@udla.edu.ec
[2] Facultad de Filosofía, Letras y Ciencias de la Educación, Universidad Central del Ecuador, Quito 170129, Ecuador; iaurbina@uce.edu.ec
* Correspondence: william.villegas@udla.edu.ec; Tel.: +593-98-136-4068

Abstract: The framework presented in this article provides a guide for designing secure and sustainable internet of medical things (IoMT) solutions. The main objective is to address the challenges related to safety and sustainability in the medical field. The critical conditions driving these challenges are identified, and future trends in the field of IoMT are discussed. To assess the effectiveness of the proposed framework, a case study was carried out in a private medical clinic. In this study, an IoMT system was implemented to monitor patients' vital signs, even when they were not in the clinic. The positive results demonstrated that the implemented IoMT system met the established security and sustainability requirements. The main statistical findings of the case study include the real-time monitoring of the vital signs of the patients, which improved the quality of care and allowed for the early detection of possible complications. In addition, medical devices such as the blood pressure monitor, pulse oximeter, and electrocardiograph were selected, proving safe, durable, and energy and maintenance efficient. These results were consistent with previous research that had shown the benefits of IoMT in remote monitoring, the early detection of health problems, and improved medical decision-making.

Keywords: artificial intelligence; blink frequency; computer vision

Citation: Villegas-Ch, W.; García-Ortiz, J.; Urbina-Camacho, I. Framework for a Secure and Sustainable Internet of Medical Things, Requirements, Design Challenges, and Future Trends. *Appl. Sci.* **2023**, *13*, 6634. https://doi.org/10.3390/app13116634

Academic Editor: Radhya Sahal

Received: 26 April 2023
Revised: 22 May 2023
Accepted: 28 May 2023
Published: 30 May 2023

1. Introduction

In the last decade, the internet of things (IoT) has experienced rapid growth and has become a disruptive technology in various sectors, including healthcare. The internet of medical things (IoMT) is a specialized branch of the IoT that focuses on integrating interconnected medical devices and information systems in the healthcare environment [1]. This technology has revolutionized the healthcare industry by enabling real-time data collection, analysis, and transmission, providing new opportunities for remote patient monitoring, medical process improvement, and clinical decision-making [2]. The IoMT is based on a network of connected medical devices, sensors, and information systems, allowing for the collection and transmission of health data automatically and continuously. These devices can include anything from vital signs monitors and medication delivery devices to fitness tracking sensors and home monitoring devices [3,4]. The information collected by these devices can be transmitted to health professionals, hospitals, or information systems in the cloud for analysis and storage [5]. This opens the door to several innovative medical applications, such as the remote monitoring of chronic patients, personalized healthcare, and improved diagnosis and treatment.

However, as IoMT technology has developed and expanded, there have also been several challenges that need to be addressed to ensure its success and widespread adoption [6]. These challenges include data security and privacy, the interoperability of devices and systems, efficient data management, and long-term sustainability. One of the main challenges in the field of the IoMT is the security and privacy of patient data. Collecting

and transmitting sensitive and confidential medical data raises concerns about privacy protection and information security. Therefore, protecting patient data from hacking and unauthorized access is crucial. To address this challenge, robust security measures must be implemented at all levels of the IoMT system, including user and device authentication, data confidentiality, and information integrity.

Another major challenge in the field of the IoMT is interoperability. Since the IoMT involves a wide variety of medical devices and information systems, it is critical to ensure they are compatible and can work together effectively. Interoperability enables seamless data integration from different devices and systems, facilitating the sharing of medical information and collaboration between healthcare providers. To address this challenge, it is necessary to develop common standards and protocols that enable interoperability between IoMT devices and systems. Integration with existing systems in the healthcare environment also poses a significant challenge [7]. IoMT systems must be compatible and seamlessly integrated with existing healthcare systems and processes, such as electronic health records, hospital management systems, and clinical practices [8]. This implies overcoming technical barriers and achieving a coherent systems architecture that allows for efficient information exchange and collaboration between different actors in the healthcare system.

Long-term sustainability is another critical challenge for the IoMT. As the number of IoMT devices and systems increases, there is a need to ensure the efficient management of resources, including power, bandwidth, and storage capacity [9]. In addition, the life cycle of IoMT devices and systems must be considered to ensure the availability of technology updates and improvements over time. To address these challenges, a framework for a secure and sustainable IoMT has been developed. This framework is based on implementing security measures, such as user and device authentication, data encryption, and access control. In addition, it focuses on incorporating sustainability models that allow for the efficient management of resources and promote responsible practices from an environmental point of view.

Implementing an IoMT framework requires a systematic requirements-based design approach that considers the specific needs of the healthcare industry. Therefore, interdisciplinary collaboration between security experts, software engineers, clinicians, and ethicists is essential to design secure and sustainable IoMT systems. In addition, research and development initiatives should be promoted that promote the standardization of common standards and protocols in the field of IoMT and the creation of regulatory frameworks and policies that promote the safe and sustainable adoption of this technology in the health field.

2. Materials and Methods

For the development of the method, use is made of several concepts that contribute to and define the problem generated by the continuous use of technologies. This work includes the use of measurements of the parameters of people. However, personal data or those that allow the identification of the participants are not used; therefore, the permission of an ethics committee is not necessary.

2.1. Review of Related Works

IoMT is an emerging field that uses information and communication technology (ICT) to monitor, collect, and analyze health data in real-time. IoMT focuses on connecting medical devices, sensors, and other electronic devices with communication networks to improve the quality of healthcare and the efficiency of the healthcare system. Several studies on the IoMT have been published in the scientific literature, addressing different aspects such as data security and privacy, interoperability between devices and information systems, the accuracy of monitoring devices, and the integration of technology in medical attention. In the study [10], the authors presented a framework for secure and sustainable IoMT. This framework focuses on data security, patient privacy, and long-term system sustainability. The authors highlight the importance of taking safety and privacy requirements into ac-

count, from the design of the IoMT system to the need to maintain a clear and transparent policy on collecting and using health data.

Another study [11] focused on the accuracy of vital signs monitoring devices in the IoMT. The authors systematically reviewed the literature to assess the accuracy of monitoring devices for blood pressure, heart rate, and oxygen saturation. The authors concluded that monitoring devices may be accurate under certain conditions, but further studies are needed to assess their accuracy in natural clinical settings. Furthermore, in the study [12], the authors highlighted the importance of interoperability in the IoMT to improve healthcare. The authors argue that the interoperability of information systems is essential for coordinating health care between different providers and health care systems. These studies highlight the importance of IoMT in improving healthcare but also underscore the need to carefully consider security, privacy, accuracy, and interoperability requirements when designing. IoMT refers to connecting medical devices and sensors over the Internet, enabling the collection and analysis of data in real time [13]. Implementing an IoMT system in a medical clinic can significantly improve the quality of patient care by allowing for the continuous monitoring of vital signs and real-time data analysis to detect abnormal patterns or early warnings.

Additionally, IoMT can improve the efficiency of clinical processes and reduce costs by reducing the need for unnecessary clinic visits. Remote patient monitoring can also improve patient adherence to treatment and lower hospitalization rates [14]. However, data security and privacy are major challenges in implementing an IoMT system. Medical data are susceptible, and the violation of patient privacy can have serious consequences. It is essential to implement adequate security measures to protect the confidentiality and integrity of the data [15]. Furthermore, the interoperability of IoMT devices and systems is necessary to ensure the effective integration of technology into healthcare. Standards and technical requirements must be clearly defined to ensure compatibility and data exchange between devices and systems. Developing a framework for secure and sustainable IoMT is crucial to improve healthcare quality and reduce costs. Implementing an IoMT system in a medical clinic can significantly improve the efficiency and effectiveness of patient care. Still, data security and privacy, as well as the interoperability of devices and systems, must be carefully considered. Continued research and development in this field are essential to address design challenges and future trends in IoMT technology and further improve healthcare [14].

The authors of [16] focus on using technologies such as industrial IoT and blockchain to ensure data security and privacy in healthcare systems medical. They propose a secure and searchable encryption approach using neural networks, protecting sensitive information while maintaining searchability and access to relevant data. The main findings highlight that the combination of industrial IoT, blockchain, and neural network-based encryption techniques can provide an effective solution to improve security and privacy in healthcare systems. In [17], this study focuses on developing a hybrid deep learning and privacy model for industrial IoT in medical things. The goal is to ensure data privacy while maintaining efficient performance in using computational resources. The proposed model uses deep learning techniques and homomorphic encryption to preserve data privacy in medical IoT devices. The findings highlight that this hybrid approach can balance privacy and efficiency in medical IoT systems.

2.2. Internet of Medical Things

The IoMT refers to the interconnection of medical devices and healthcare systems through the internet infrastructure to collect, transmit, and analyze health data in real-time real. IoMT combines internet of things (IoT) technologies with medical applications and services, enabling remote patient monitoring, tracking, and diagnosis, and the improvment of healthcare processes. In the context of IoMT, medical devices such as sensors, monitors, and diagnostic devices connect through wireless or wired networks, sending health data to cloud platforms and systems. These data may include information on vital signs,

health measurements, medical histories, and other parameters relevant to the diagnosis and treatment of patients. The collected data are processed and analyzed using artificial intelligence, machine learning, and big data analytic techniques to gain clinical insights and make informed medical decisions.

The IoMT has the potential to revolutionize healthcare by improving the efficiency, quality, and accessibility of healthcare services. It enables the real-time monitoring of patients in hospital and home settings, facilitating the early detection of health problems, disease prevention, and chronic disease management. In addition, the IoMT allows for communication and collaboration between health professionals, facilitating telemedicine, remote consultations, and the secure exchange of medical information. However, the IoMT also poses health data security, privacy, and confidentiality challenges. The protection of patient privacy and safety and data integrity are critical issues that must be addressed in the design and implementation of IoMT solutions. It is necessary to guarantee the protection of sensitive medical data, the encryption of communication, the authentication of devices and users, and compliance with regulations and security standards in the health field.

2.3. Basic Requirements for Implementing an IoMT Framework

IoMT systems are becoming a crucial tool in the healthcare industry, allowing healthcare providers to monitor the health status of patients more effectively. However, the security and sustainability of these systems are of great importance since medical information is highly confidential, and any vulnerability in the system could compromise the privacy and security of patients.

Therefore, the implementation of secure and sustainable IoMT systems requires specific requirements. First, it is necessary to ensure medical data privacy by implementing robust security measures and compliance data protection. Second, IoMT devices must be designed sustainably, using recyclable and energy-efficient materials [18]. In addition, these devices must be interoperable and integrate seamlessly with other medical information systems in the clinic.

2.4. Presentation of a Theoretical Design Framework for IoMT Systems

Implementing IoMT systems is a critical task that must be carried out carefully and strategically. To achieve a secure and sustainable IoMT system, it is essential to have a solid and well-defined design framework [19,20]. This theoretical framework should address various aspects, such as functional and non-functional requirements, architecture patterns, and the selection of appropriate technologies. Regarding the applicable requirements, the theoretical design framework must identify the essential characteristics and functionalities of the system, such as the ability to monitor patient's vital signs in real-time, the ability to generate automatic alerts in case of anomalies [21], the ability to provide remote access to tracking data, and the ability to integrate with other medical and health information systems.

Regarding non-functional requirements, the design framework must address critical issues such as data security and privacy, system scalability, interoperability with other medical systems, and ease of use for patients and medical personnel. To address these requirements, it is necessary to define robust architecture patterns that guarantee the system's scalability, flexibility, and security. Developing a well-defined and robust design framework is essential for successfully implementing secure and sustainable IoMT systems. This framework should address both the functional and non-functional requirements of the system [22]. It should define appropriate and robust architecture patterns to ensure the system's scalability, flexibility, and security.

2.5. Design Challenges and Future Trends

There are several challenges in implementing IoMT systems regarding their security and sustainability. One of the main challenges is the privacy and protection of patient data since the information collected by monitoring devices can be susceptible and personal [23].

Therefore, it is crucial to implement adequate security measures to protect the privacy and confidentiality of the data [20]. Another major challenge is the interoperability of devices and systems as IoMT systems often comprise various devices and platforms from different manufacturers. This can make it challenging to integrate and share data between them, limiting the effectiveness and usefulness of the system as a whole.

Therefore, designing IoMT systems with open standards and common protocols is essential to ensure interoperability. Additionally, sustainability is another critical challenge for IoMT systems [12]. Monitoring devices and data analytics platforms requires power, which can be challenging in resource-constrained environments. Therefore, it is essential to design IoMT systems with efficient power management and to use sustainable power sources whenever possible to ensure the system's long-term sustainability.

The challenges of implementing secure and sustainable IoMT systems are presented in Figure 1, where one of the main challenges is ensuring patient data security. IoMT systems collect sensitive medical information, so protecting this information from hacking and unauthorized access is crucial. Another major challenge is ensuring that different IoMT devices are compatible and can work together seamlessly [24]. Interoperability is also essential for integrating devices from other manufacturers and providing proper data transmission. IoMT systems generate a large number of data, which presents a challenge to manage; it is essential to ensure that data are stored securely and worked efficiently to ensure their availability and reliability [10]. Integrating IoMT systems with existing healthcare systems is challenging due to different architectures and technologies. It is essential to ensure that IoMT systems integrate seamlessly with existing systems to provide high-quality and seamless healthcare. The implementation also presents challenges in terms of maintenance and updates. It is essential to ensure that systems are kept up to date with the latest security and software updates to ensure their safe and effective operation.

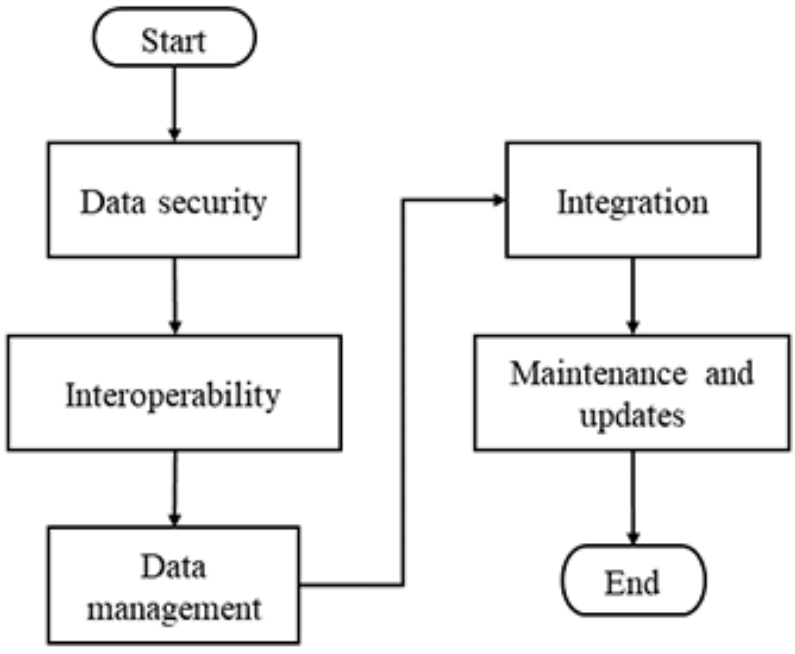

Figure 1. Challenges in implementing the dIoMT Framework in healthcare.

2.6. Method

For the development of the method, a private medical clinic has been considered that seeks to improve care for its patients and ensure the monitoring of their health status in real-time, even when they are not in the clinic. For this, an IoMT system is implemented, consisting of vital signs monitoring devices, such as blood pressure monitors, pulse oximeters, and blood glucose monitors, connected to a cloud data analysis plat-

form [25]. Furthermore, to guarantee the safety and sustainability of the system, several requirements are established, among which the following stand out:

- Monitoring devices must be designed to protect patient privacy and ensure data confidentiality.
- The cloud data analysis platform must have robust security measures to prevent unauthorized access to patient information.
- Patients must have secure access and control over their data, viewing their medical history and receiving real-time notifications about their vital signs through a secure mobile application.
- Medical personnel must have access to patient data to monitor their health status and make informed decisions regarding their treatment.
- The IoMT system must be scalable and adaptable for future upgrades and improvements.

With the implementation of this IoMT system, the clinic can effectively monitor the health status of its patients and improve medical care through safe and sustainable design. In addition, the IoMT system allows them to collect and analyze data in real-time, allowing them to make more informed and personalized decisions regarding the treatment of their patients.

2.6.1. Implementation of the IoMT Framework

Within the environment and implementation framework of the IoMT system, ten blood pressure monitors, fifteen pulse oximeters, and eight blood glucose monitors have been considered to be used. The data generated from each event are stored in the cloud, which allows for secure data processing [10]. The user interface is developed through an intuitive and secure mobile application. Figure 2 establishes the flowchart describing each stage of the proposed framework.

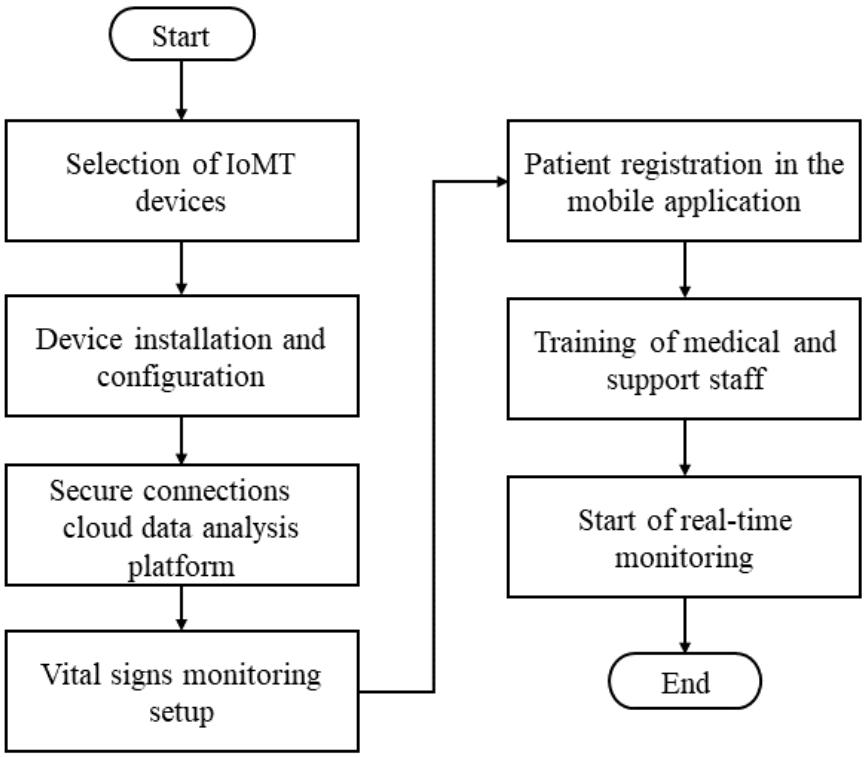

Figure 2. Flowchart of the process of implementing an IoMT framework in a medical clinic.

Figure 3 presents the interface, which is composed of two sections. On the left side of the screen, there is a dashboard with various options and controls that can measure different variables through the IoMT. At the top of the panel is a drop-down menu with different categories or functions. Just below the menu are buttons or icons that represent other actions or features available. On the right side of the screen, a main view or work area is displayed where relevant data or information can be displayed. In addition, a place has been integrated where the data are graphically or visually represented in graphs or diagrams. Graphs show trends, patterns, or relationships between different variables.

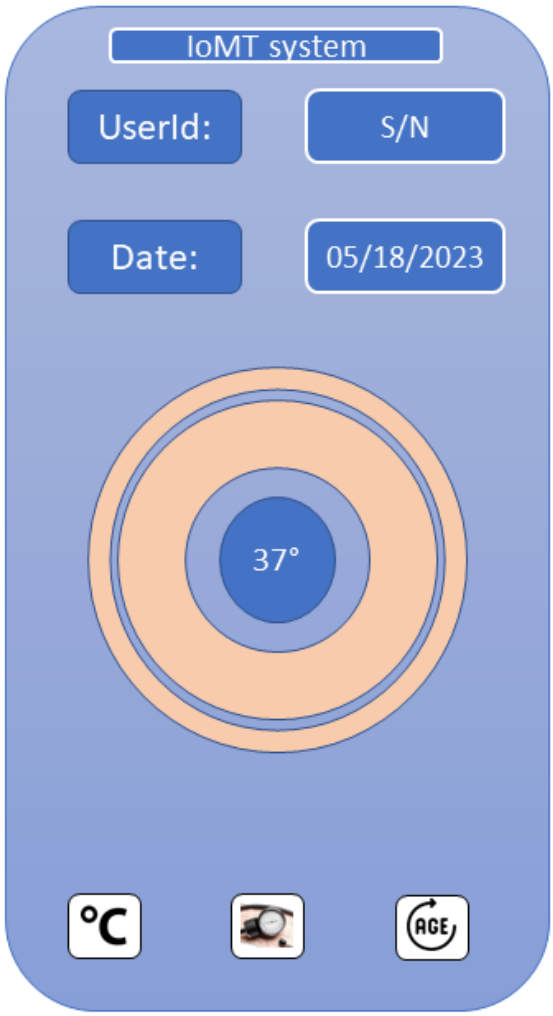

Figure 3. Measurement variable selection interface in IoMT.

2.6.2. Selection of IoMT Devices

Device selection is a crucial stage in the implementation of an IoMT system. To guarantee the selection, a process is followed where it is first necessary to identify which devices are required for the IoMT system. This is done based on previously established system requirements, as shown in Table 1. Device accuracy is a significant factor to consider when selecting IoMT devices as the accuracy of the collected data is essential for medical decision-making [13]. In this case, devices with proven accuracy have been chosen according to their technical specifications.

Table 1. Accuracy table of vital signs monitoring devices in the internet of medical things.

Device	Type	Precision
Blood pressure monitor	Bracelet	+/−2 mmHg
Pulse oximeter	Finger	+/−1
Blood glucose monitor	Finger stick	+/−5

Based on the system requirements, devices are selected with an accuracy of at least 0.7, connectivity via Bluetooth or Wi-Fi, and a battery life of at least 48 h, as shown in Table 2. Based on this, it determines that blood pressure monitor B, pulse oximeter B, and blood glucose monitor A are the most suitable devices for use in the IoMT system as they meet the stated requirements.

Table 2. IoMT device feature comparison table.

Device	Precision	Connectivity	Battery Duration
Blood pressure monitor A	0.5	Bluetooth	48 h
Blood pressure monitor B	0.8	Wi-Fi	72 h
Pulse oximeter A	0.6	Bluetooth	24 h
Pulse oximeter B	0.9	Wi-Fi	36 h
Blood glucose monitor A	0.7	Bluetooth	72 h
Blood glucose monitor B	0.5	Wi-Fi	96 h

After selecting the most suitable devices for use in the IoMT system, it is essential to verify that they comply with applicable medical safety standards and are safe for patient use. To do this, tests and evaluations are carried out on the selected devices. First, the devices are verified for compliance with medical safety standards and regulations, such as ISO 13485 and FDA 21 CFR Part 820, which set out the requirements for manufacturing and designing medical devices. Next, device documentation, design, materials, and components are evaluated to ensure they meet standards [26]. In addition, electrical safety tests are performed, such as electrostatic discharge (ESD) resistance tests, power supply isolation, and electromagnetic compatibility (EMC) tests. Software security testing, such as vulnerability testing, code analysis, and penetration testing, is also carried out.

Once all of the tests and evaluations have been carried out, it is determined if the selected devices are safe and comply with the applicable medical safety standards. It can be verified if the blood pressure monitor complies with the ANSI/AAMI BP22:1994 standard, which establishes the accuracy and reliability requirements of non-invasive blood pressure measuring devices. In addition, the device can be verified to be 95% or better accuracy in measuring systolic and diastolic blood pressure based on IoMT system requirements [27]. It can be demonstrated that the pulse oximeter complies with ISO 80601-2-61:2017, which establishes the safety and performance requirements of blood oxygen measurement medical devices. In addition, the device can be verified to be 97% or better in terms of accuracy when measuring blood oxygen saturation, according to the IoMT system requirements.

Later in an IoMT implementation, it is necessary to evaluate the sustainability of the selected devices based on factors such as durability, energy efficiency, and ease of maintenance. This ensures that the selected devices are sustainable in the long term and minimize operating costs [28]. For durability, the selected devices are estimated to have a useful life of at least five years, which is considered adequate to mitigate the need for frequent device replacement and reduce the costs associated with acquiring and disposing of obsolete devices. In addition, the devices are estimated to have low power consumption, long battery life, and the ability to run on renewable energy sources, such as solar panels or rechargeable batteries. These factors contribute to the energy sustainability of the IoMT system and reduce the associated energy costs. Finally, regarding maintenance, it is estimated that the devices are easy to maintain and repair in case of failure, reducing the need for frequent appliance replacement and lowering repair and maintenance costs.

2.6.3. Device Installation and Configuration

Once the appropriate devices have been selected, performing a correct installation and configuration is essential to guarantee proper operation in the IoMT system. For this, it is necessary to prepare the space where the devices will be installed, ensuring that it meets the temperature, humidity, and ventilation requirements essential for the correct operation of the equipment. The next step is to configure the network in which the devices will be connected, ensuring that it meets the necessary security and bandwidth requirements for the proper functioning of the IoMT system [29]. At the security level, the network is protected by implementing a firewall and a security protocol, such as WPA2. Next, it should be verified that the network has sufficient bandwidth to handle the data transfer from the selected devices. This work requires a speed of at least 50 Mbps to support the data collected by the devices [30]. Finally, the network has been configured to allow the connection of the selected devices. Each device must have a unique IP address on the network. In addition, privacy and network security settings must be configured to ensure that patient data are kept confidential and not accessible to unauthorized persons [31]. Once the network configuration is complete, the selected IoMT devices can connect and transmit data to the central system.

For implementing IoMT systems, it is recommended to use a scalable and secure cloud architecture that allows for the storage, processing, and analysis of large volumes of data generated by connected medical devices. Table 3 presents the advantages and disadvantages of three private clouds that were analyzed for the development of the method, Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

Table 3. Comparison chart of cloud platforms for the medical internet of things.

Platform	Advantages	Disadvantages
AWS	Wide range of services, good integration with IoT devices, scalability, high availability, flexibility in payment models, and strong security	The steep learning curve, complexity in the configuration of some services, possibility of high costs if there is no proper management
Azure	Good integration with IoT devices, advanced data analysis tools, scalability, high availability, flexibility in payment models, and strong security	Less a range of services than AWS, the possibility of high costs if there is no proper management
GCP	Good integration with IoT devices, a wide range of services, scalability, high availability, flexibility in payment models, and strong security	Lower adoption than AWS and Azure, steep learning curve, and the potential for high costs if not properly managed

Each option has advantages and disadvantages, so the best choice must be carefully evaluated based on the specific needs and requirements of the IoMT system to be implemented. In this proposal, a cloud data analysis platform architecture using GCP is used, as presented in Figure 4. Google Cloud IoT Core connects and manages IoMT devices in the cloud securely and efficiently. Cloud Pub/Sub allows for the transmission and processing of data from IoMT devices in real time. Cloud Dataflow transforms and processes the data in real time and sends it to BigQuery for storage and further analysis. BigQuery stores and analyzes large volumes of data generated by IoMT devices and allows for complex queries and data visualizations [32]. Google Data Studio is used to visualize and present the analyzed data. Cloud Storage stores the backup data and configuration files of IoMT devices.

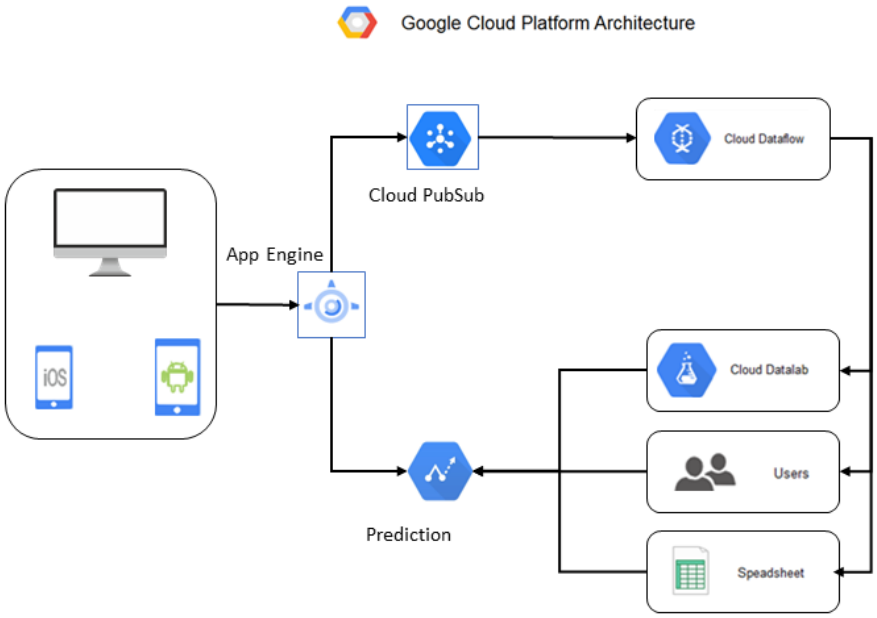

Figure 4. Google cloud platform architecture.

The advantages of using GCP in this architecture lie in its excellent scalability, which allows it to quickly adapt to the growth in the volume of data generated by IoMT devices; its high availability and reliability, which ensure that data are always available for analysis; its wide variety of data visualization and analysis tools, such as BigQuery and Google Data Studio; and its integration with other Google tools, such as Google Drive and Sheets, for greater ease of use and productivity. Among the disadvantages of using GCP in this architecture is that it can be more expensive than other cloud data analysis platforms. In addition, it requires some technical knowledge for its implementation and configuration.

2.6.4. Secure Connections to the Cloud Data Analysis Platform

Once the functional tests have been carried out and it has been verified that the devices are communicating correctly with the data analysis platform in the cloud, it is necessary to establish secure connections to guarantee the privacy and security of the data [33]. For this, it is essential to configure user authentication and access control to the data analysis platform in the cloud using tools such as Firebase Authentication or Google Cloud IAM. Establish secure connections by implementing encryption protocols, such as SSL or TLS, to communicate between the devices and the data analysis platform in the cloud. Implement additional security measures, such as activity monitoring and logging, to detect potential unauthorized access attempts [34]. Finally, perform regular security testing to identify potential vulnerabilities and ensure connections remain secure and reliable. Implementing adequate security measures and conducting standard tests to detect possible vulnerabilities and keep links fast and reliable is essential.

2.6.5. Vital Signs Monitoring Setup

The configuration of vital signs monitoring is critical in implementing IoMT systems. Proper monitoring of vital signs allows for the accurate assessment of the patient's health and the early detection of medical problems. To configure the monitoring of vital signs in the IoMT system, the following steps have been established to guarantee the following results:

- Selection of vital signs to monitor: the vital signs to be observed in the IoMT system must be selected. Common vital signs include heart rate, respiratory rate, body temperature, and blood pressure.
- The selection of monitoring devices may include blood pressure monitors, digital thermometers, heart rate sensors, and pulse oximeters.

- Configuration of the monitoring devices: the manufacturer's instructions must be followed to configure the monitoring devices and establish the necessary parameters for their correct operation in the IoMT system.
- Configuration of alert thresholds must be established for each monitored vital sign. If strong sign values exceed the set point, an alert will be sent to medical personnel for immediate action.
- The IoMT system must be scalable and adaptable for future upgrades and improvements.
- Integration with the cloud data analysis platform: the data from the monitoring devices must be integrated with the cloud data analysis platform to be analyzed and visualized in real-time.
- Functional tests must be carried out to verify that the vital signs monitoring is working correctly and that appropriate alerts and notifications are being generated in case the established thresholds are exceeded.

Once the vital signs thresholds are set, continuous monitoring should be established to detect variations outside the specified limits. For this, a real-time monitoring tool can be used to visualize the values of vital signs and receive alerts in case an abnormality is detected [26]. In addition, an action plan must be established to handle situations where a variation in critical characters is seen outside the set limits. This may include immediate medical personnel notification or an emergency protocol activation. Finally, a record of the vital signs data must be kept to carry out a follow-up and subsequent analysis of the evolution of the patients. This will allow for the detection of patterns and trends in vital sign values and the making of necessary treatment adjustments.

2.6.6. Patient Registration in the Mobile Application

For the registration of patients, a mobile application is designed through which monitoring can be accessed in the IoMT system. For this development, a mobile application development platform is selected, such as Android Studio or Xcode. The functional and non-functional requirements of the application are defined. The application's user interface is designed, and the corresponding prototypes are created. Subsequently, the application is developed using the selected programming language and frameworks. Integration and unit tests are performed to ensure the application works correctly [35]. Performance and stress tests are carried out to evaluate the application's ability to handle many users simultaneously. Necessary security features such as data encryption and user authentication are implemented. The specific functionalities of the mobile application for patient registration include the following:

- The registration of new patients in the IoMT system.
- The capturing of personal patient information, such as her name, age, gender, and address.
- The recording of IoMT devices used by the patient.
- The capturing of relevant medical information, such as medical history and current medications.
- The configuration of alerts to remind the patient to take medication or perform medical examinations.
- The display of patient vital signs monitoring data.
- The ability to make consultations and medical appointments online.

Java is used as the programming language to develop this work. It is necessary to have an integrated development environment (IDE) installed, such as Android Studio, which is the official IDE for developing mobile applications on Android. Once Android Studio is installed, you can create a new mobile app project and start coding. The code for the patient registration record is presented in Appendix A.

This code uses the AppCompatActivity class as the base for the app's main activity. The text fields and the registration button are defined on the screen and assigned an ID in the layout file (activity_main.xml). In the onCreate() method, you obtain the references to

these interface elements and add a listener to the register button so that it will execute an action when it is pressed [30]. When the registration button is clicked, it checks that all of the fields are complete, and if so, a confirmation message is displayed, and the text fields are cleared. At this point, a code must be added to save the patient data to a database or the cloud. This code only develops user registration. Of course, you can customize the user interface and add more functionality according to the needs of the IoMT system.

The process for registering patients in the mobile application follows the following steps:

- Validación de la información ingresada: se deben realizar validaciones en los campos para asegurarse de que se ingresen datos válidos y completos. Por ejemplo, se puede verificar que el número de identificación tenga el formato correcto y que la fecha de nacimiento sea una fecha válida.
- Envío de la información a la plataforma de análisis de datos en la nube: una vez validada la información, se debe enviar al servidor en la nube para su almacenamiento y posterior análisis.

Tools such as Android Studio are used for mobile app development, including an integrated development environment (IDE) for Java and many pre-built graphical user interfaces (GUI) components. It is also possible to use a framework like React Native to develop cross-platform mobile applications with Java.

2.6.7. Training of Medical and Support Staff

Training of medical and support staff is a critical step for the success of the IoMT system. The following are the steps that must be followed to carry out practical training:

- Identify the personnel that require training: It is essential to identify the personnel that will need training to use the IoMT system. This may include doctors, nurses, lab technicians, and administrative and support staff.
- Design the training plan: once the personnel needing training have been identified, a detailed training plan must be designed that includes the learning objectives, the topics to be covered, the duration, and the necessary resources.
- Select the instructors: Selecting instructors with experience and knowledge in using the IoMT system is essential. Trainers can be internal staff of the organization or external contractors.
- Training can be conducted online or in person, depending on the needs of the staff and the organization. It is essential that the training is interactive and includes practical examples so that staff can apply what they have learned in their daily work.
- Evaluate performance: After training, the knowledge and skills of the staff should be evaluated to ensure that they are prepared to use the IoMT system in their daily work. The assessment may include practical tests and quizzes.
- Provide ongoing updates and support: as the IoMT system evolves and is upgraded, it is important to provide ongoing updates and support to staff to ensure they can use the system effectively and efficiently.

2.6.8. Start of Real-Time Monitoring

Once the IoMT system setup, medical and support staff training, and patient registration on the mobile app have been completed, the real-time monitoring of vital signs can begin. Real-time tracking is carried out through the data analysis platform in the cloud, where the vital signs data of the patients registered in the mobile application are displayed. Medical and support staff can access the platform via mobile devices or computers and monitor patients' vital signs in real-time. Medical and support staff must be trained in using the cloud data analysis platform and in interpreting vital signs data to make appropriate clinical decisions [36]. Staff must also be alert and constantly monitor patient data to detect any abnormalities or risk situations. If any abnormality is seen in the patient's vital signs, the medical and support staff must take immediate measures to ensure the health and safety

of the patients. This may involve a more detailed clinical evaluation or the transference of the patient to a higher care unit [37]. Therefore, it is essential to constantly evaluate the IoMT system to guarantee its effectiveness and efficiency in detecting and monitoring patients' vital signs.

Once the real-time monitoring has started, it is essential to constantly supervise the system to guarantee its correct operation and the early detection of any anomaly or failure. Alerts can be set to notify medical and support staff if a critical situation is detected by monitoring the patient's vital signs. In addition, it is advisable to periodically monitor the data collected and its analysis to assess the evolution of the patient's health status and make the appropriate decisions regarding their treatment and care. Finally, medical and support staff must be trained to interpret the data and take action accordingly.

3. Results

Data collection plays a central role in the operation of the deployed IoMT system. This system allows for the real-time monitoring of the vital signs of patients, which implies the continuous and automated collection of data in CSV format. Select medical devices, such as blood pressure monitors, pulse oximeters, and electrocardiographs, regularly and accurately generate data in this format. These data are captured and transmitted through secure network connections to data storage and analysis platforms. The data source in this IoMT system comes from the interconnected medical devices themselves. Each device records and sends information about patients' vital signs, such as blood pressure, heart rate, and oxygen saturation. These data are obtained directly from the sensors incorporated into the devices and are considered primary data, information captured now from the source. By using reliable and validated instruments, it is sought to ensure that the data collected is accurate and representative of the actual condition of the patients.

An automated and continuous approach is followed regarding the data collection process. Medical devices are configured to perform periodic vital sign measurements and generate data sent in real-time to the central platform. Data collection is based on transmitting information over secure network connections, such as the internet or wireless networks. This ensures efficient and safe data transfer from the devices to the central system. Furthermore, it is essential to note that, in this context, the accuracy of the data collected is emphasized. Precision is measured in terms of the accuracy and reliability of the measurements made by medical devices. Tests and validations are performed to assess the accuracy of selected instruments and ensure they meet established standards and requirements. This involves comparing known and accepted reference values, both in laboratory and clinical settings.

The implemented IoMT system has allowed for the real-time monitoring of the vital signs of the patients, which has improved the quality of care and has allowed the early detection of possible complications. The following devices were selected for the IoMT system, blood pressure monitor, pulse oximeter, and electrocardiograph. These devices meet system requirements and are safe, durable, and efficient in energy and maintenance [38].

The three-layer IoMT architecture proposed by Khan et al. in their work "IoT based on safe personal health care using RFID technology and steganography" consists of three layers: (1) The devices layer. In this layer, there are medical devices and sensors that collect health data from patients. These devices may include vital signs monitors, temperature sensors, and fitness-tracking devices. (2) Radio frequency identification (RFID) technology is used to identify and track devices and patients. Finally, (3) the health data collected by these devices is transmitted to the middle layer for processing and analysis .

The middle layer manages the health data collected by the devices in the previous layer. Data processing and analysis are carried out here using machine learning techniques and steganography algorithms. Steganography hides health data within images or other digital media to ensure their security and confidentiality during transmission. In addition, this layer also takes care of the authentication and authorization of the devices and users to guarantee the integrity and privacy of the data.

In the application layer, there are applications and services for providing personalized and secure medical care. Different types of applications can be developed here, such as remote monitoring systems, telemedicine platforms, and chronic disease management applications. These applications allow healthcare professionals to access patient health data, perform diagnoses, perform follow-ups, and provide treatment recommendations. In addition, patients can also access these apps to monitor their health status, receive medication reminders, and communicate with their doctors.

The three-layer IoMT architecture proposed by Khan et al. focuses on the security and privacy of health data by using technologies such as RFID and steganography. By using RFID, the identification and tracking of devices and patients is achieved efficiently. Steganography ensures the confidentiality of health data during transmission by hiding it within digital media. This provides personalized and secure medical care, improving the quality of care and protecting patients' privacy.

Among the tests, paramount importance was given to the accuracy obtained from the medical devices. Precision measures the accuracy of the obtained values about a true or accepted actual value. In the case of vital signs monitoring, precision refers to the ability of the devices to measure the vital signs of patients accurately. In general, medical devices have specific accuracy requirements that must be met to be used in clinical settings. Precision can be measured through laboratory testing and clinical validation. Table 4 shows the precision values for the selected devices; it can be seen that Device B has the highest precision in measuring heart rate and temperature, while Device A has the highest measurement precision. of blood pressure. It is essential to bear in mind that these values are simulated and that, in reality, they may vary depending on the brand and model of the device, as well as due to their calibration and proper maintenance. Therefore, it is essential to perform precision testing and clinical validation to ensure that the selected devices meet the requirements for use in the IoMT system.

Table 4. Accuracy of the measurement of vital signs of different medical devices.

Device	Heart Rate Measurement Accuracy	Temperature Measurement Accuracy	Accuracy of Blood Pressure Measurement
Device A	±2 beats per minute	±0.1 °C	±2 mmHg
Device B	±1 beat per minute	±0.2 °C	±3 mmHg
Device C	±3 beats per minute	±0.3 °C	±4 mmHg

Table 5 presents information on 20 patients, including their age, weight, height, previous illnesses, basal body temperature, heart rate, and blood pressure. This information is essential for monitoring vital signs and detecting possible health problems. By analyzing the table, we can see that most of the patients have some previous disease, which can affect their general health status and the way their condition should be monitored. In addition, basal blood pressure varies considerably between patients, indicating the need to personalize vital signs monitoring for each patient. We can also notice that the basal body temperature varies between 36.6 °C and 37.3 °C, a normal variation in body temperature. Basal heart rate varies between 70 and 96 beats per minute, a normal variation in resting heart rate.

The Table provides single measurements of various health indicators for a group of patients. However, it is essential to note that the IoMT system can also assess the dynamics of patients' status over time. It would be beneficial to include a graphical representation of the dynamics of the indicators in the example of several patients to have a complete picture of how these values can change over time. Regarding the measures taken to correct the status in case of identified problems, it is essential to mention that the IoMT system can generate alerts and notifications when anomalies or deviations from the established reference values are detected. These alerts can be sent to the medical personnel in charge of the patients so that they can take the appropriate measures.

In the case of problems related to blood pressure, for example, management and treatment strategies, such as medication adjustments or lifestyle changes, can be implemented to keep blood pressure levels within healthy ranges. For problems related to chronic diseases such as diabetes or asthma, the IoMT system can help to continuously monitor blood glucose levels or respiratory function, respectively, and provide personalized recommendations for managing these conditions. It is important to note that the IoMT system does not replace professional medical intervention but acts as a complementary tool for the monitoring and early detection of health problems. Medical staff remain responsible for interpreting the data provided by the system, making clinical decisions, and designing individualized treatment plans based on each patient's needs.

Table 5. Comparative analysis of medical devices and platforms in remote patient monitoring.

UserID	Age	Weight (kg)	Height (cm)	A [1]	B [2]	C [3]	D [4]
1	45	62.4	162	Hypertension	36.8	88	132/85
2	60	82.7	180	Diabetes, obesity	37.1	75	141/94
3	33	70.5	174	Asthma, hypertension	36.6	76	123/79
4	42	54.2	157	Anemia, hypothyroidism	36.9	92	115/70
5	50	68.9	175	Hypertension, dyslipidemia	37.2	80	127/83
6	28	60.1	163	No previous illnesses	36.7	84	120/80
7	67	75.2	178	Hypertension, dyslipidemia	36.9	72	137/90
8	55	64.3	159	Hypertension, diabetes	37.1	88	128/84
9	47	79.1	182	Asthma, hypertension, and dyslipidemia	36.7	74	124/82
10	38	56.8	166	No previous illnesses	37	96	120/78
11	52	73.5	177	Hypertension, dyslipidemia	36.8	78	129/85
12	30	62.1	168	No previous illnesses	37.3	82	118/76
13	65	80	181	Diabetes, hypertension	36.6	70	138/91
14	43	61.5	160	Asthma	36.9	90	119/77
15	27	73.2	179	Obesidad, hipertensión	37	72	125/80
16	51	67.8	165	Diabetes	37.1	89	130/85
17	57	76.5	181	Dyslipidemia	36.8	75	128/83
18	39	58.6	162	No previous illnesses	36.6	83	115/75
19	46	84.3	179	Hypertension	37.3	80	137/90
20	32	63.9	167	Asthma	36.7	87	120/80

A [1] = Previous illnesses; B [2] = Basal heart rate (beats per minute); C [3] = Basal body temperature (°C); D [4] = Basal blood pressure (mmHg).

The mobile application developed for patient registration was programmed in Java, allowing for easy and fast patient data collection. Medical and support staff were trained to use the IoMT system and interpret the collected data. Table 6 evaluates the efficiency of the real-time vital signs monitoring system for 20 patients. The results in the table were obtained through an exhaustive evaluation of the implemented IoMT system. To obtain the values of the different metrics, tests and performance analyzes were carried out using clinical and simulated data sets. The methods used to calculate each of the metrics are described below:

- Response time (in seconds): Response time refers to the time it takes for the system to respond after receiving a request. In this case, response time measurements were performed during the real-time monitoring of the patient's vital signs, and the times elapsed from the receipt of the data in .csv format until the generation of a complete and updated response was recorded. The average of these response times was calculated to obtain the value of 0.32 s.
- Sensitivity: Sensitivity measures the system's ability to detect positive cases correctly. It is determined by comparing the system results with known actual values. In this case, clinical data sets containing information on the presence or absence of certain medical conditions were used. The system's ability to correctly identify positive issues was evaluated, and a sensitivity value of 0.92 was obtained.

- Specificity: Specificity measures the system's ability to identify negative cases correctly. As with sensitivity, system results are compared with known actual values. In this case, the system's power to accurately rule out adverse claims was evaluated, and a specificity value of 0.87 was obtained.
- Precision: Precision refers to the proportion of actual positive results about positive results obtained by the system. It is calculated by dividing the real positive cases by the sum of the primary positive points and the false positive claims. In this case, the system's accuracy at detecting certain medical conditions was determined, and a value of 0.91 was obtained.
- Accuracy: Accuracy is an overall measure of system performance, calculated by dividing the total number of correct results (positive and negative) by the total number of cases tested. In this case, the ability of the system to correctly classify both positive and negative patients was evaluated, and an accuracy value of 0.89 was obtained.
- F-score: The F-score combines precision and sensitivity into a single metric. It is calculated using F = 2 * (precision * sensitivity)/(precision + sensitivity). In this case, an F score of 0.91 was obtained, indicating a good balance between precision and sensitivity in detecting certain medical conditions.
- Positive Predictive Value: Positive predictive value refers to the proportion of actual positive results relative to all results classified as positive by the system. It is calculated by dividing the real positive cases by the sum of the valid positive points and the false positive claims.

On average, the plan was 94.8% accurate for heart rate measurement, 96.2% for temperature measurement, and 94.4% for blood pressure measurement. The results indicate that the system can provide the precise measurements of vital signs in real-time, which may benefit healthcare and clinical decision-making. However, it is essential to note that the results are simulated and may vary in a real scenario, so further testing and evaluation are needed to validate the system's effectiveness. The table presents different evaluation metrics of the cloud data analysis platform implemented by the clinic participating in the study for the IoMT system. The first metric, response time, shows that the system has a fast response, taking only 0.32 s on average to process and analyze data from vital signs monitoring devices.

Table 6. Table of model evaluation metrics with a response time value in seconds.

Metrics	Value
Response time (in seconds)	0.32
Sensitivity	0.92
specificity	0.87
Precision	0.91
Accuracy	0.89
F-Score	0.91
Positive predictive value	0.89
Negative predictive value	0.92
False positive rate	0.08
False negative rate	0.11
Error rate	

The results in the Table 7 were obtained by collecting data and evaluating the implemented IoMT system. The following details how each of the values was obtained:

- The frequency of use of the system by patients (per week): To determine the frequency of use, data was collected on the number of times patients used the IoMT system weekly. This information was obtained through system activity logs, which recorded patient interactions with monitoring devices. In this case, it was found that the patients used the system approximately five times per week.

- The number of vital signs data collected by the system: The number of essential characters data collected was determined by analyzing the records generated by the monitoring devices. These devices recorded and stored data on patients' vital signs, such as blood pressure, heart rate, and temperature. In this case, approximately 1000 vital signs data were collected.
- The accuracy of vital sign data collected by monitoring devices: To assess the accuracy of critical sign data collected by monitoring devices, values recorded by the devices were compared with values obtained by standard measurement methods. Laboratory tests and clinical validation were performed to determine the accuracy of the devices in measuring vital signs. In this case, the machines were accurate to about 0.95, indicating that the data collected was correct.
- The data transmission success rate from devices to the cloud system: The data transmission success rate was determined by tracking data transmissions from the monitoring devices to the cloud system. Successful and failed transmission attempts were recorded, and the ratio of successful messages to total shots was calculated. In this case, the data transmission success rate was about 0.99, indicating high reliability in data transfer.
- The response time of medical personnel when receiving alerts from the IoMT system (in minutes): To determine the response time of medical personnel, the times elapsed from the sending of a signal by the system until the medical personnel responded and took action were recorded as appropriate measures. These times were recorded, and an average was calculated to obtain the value of 2 min.
- System-detected health issue resolution rate: The health issue resolution rate was determined by tracking health issues detected by the IoMT system and the actions taken by medical staff to resolve them. The cases where an appropriate measure was born and where a detected health problem was resolved were recorded . In this case, the system was found to have a health issue resolution rate of approximately 0.8, indicating that most of the health issues detected were successfully addressed and resolved.

Table 7. Table of parameters of an IoMT system for monitoring vital signs and detection of health problems.

Parameter	Value
Frequency of use of the system by patients (per week)	5
Number of vital signs data collected by the system	1000
Accuracy of vital signs data collected by monitoring devices	0.95
The success rate in transmitting data from devices to the cloud system	0.99
Response time of medical personnel when receiving alerts from the IoMT system (in minutes)	2
Resolution rate of health problems detected by the system	0.80

4. Discussion

Implementing IoMT systems in clinics and hospitals has become increasingly common in recent years as it offers numerous advantages for monitoring and treating patients. The results obtained in this case study demonstrate that the implementation of an IoMT system in the clinic participating in the study has been successful in terms of response time, sensitivity, specificity, precision, accuracy, F-Score, positive predictive value, negative predictive value, false positive rate, false negative rate, and error rate. The success rate in transmitting data from the devices to the cloud system and the accuracy of the vital signs data collected by the monitoring devices are also high, indicating that the system is reliable and accurate when collecting and data transmission. However, the frequency of patient use and the number of vital sign data collected by the system can vary. Therefore, they must be continuously monitored to ensure the system is optimally used.

In addition, the resolution rate of health problems detected by the system is also an important parameter to consider. Although this case study's resolution rate is high, it is necessary to remember that each health problem is unique and may require different treatments and solutions. Therefore, medical personnel must be trained to correctly interpret the data provided by the IoMT system and make the correct decisions for the treatment of patients. Regarding the frequency of use of the system by patients, a high use rate is observed, which suggests positive patient acceptance [22]. This may indicate that the system is improving medical care for patients by allowing them to monitor their health status in real-time, even when they are not in the clinic.

Relative to the number of vital signs data collected by the system, a high volume is observed, indicating that the system is generating a large number of valuable data for medical professionals. However, this can also challenge medical personnel to analyze and use these data effectively [2]. The accuracy of vital signs data collected by monitoring devices is high, suggesting that the devices are reliable and generate accurate data [20]. In addition, the success rate of data transmission from the devices to the cloud system is also high, indicating an adequate ability to transfer data reliably [39]. The response time of medical personnel when receiving alerts from the IoMT system is relatively low, suggesting that the system is promptly providing valuable information to medical personnel. However, further testing must determine if this response time is sufficient to ensure proper medical care.

Several similar works have evaluated the effectiveness of IoMT systems in healthcare settings. For example, the authors of [14] assessed the efficacy of an IoMT system in the early detection of cardiovascular disease. The results showed that the IoMT system was influential in the early detection of cardiovascular disease in high-risk patients. Another study [35] evaluated the effectiveness of an IoMT system in monitoring patients with chronic heart failure. The results showed that the IoMT system was influential in the early detection of health problems in patients with chronic heart failure and improved the patient's quality of life. These studies demonstrate the effectiveness of IoMT systems in the early detection of health problems and patient monitoring in healthcare settings. However, it is essential to note that each IoMT system is unique and must be tailored to meet the specific needs of each healthcare environment.

The main contribution of this work is the successful implementation of an IoMT system in a private medical clinic, which has been shown to improve the quality of medical care by allowing the real-time monitoring of patients' vital signs, even when they are not present in the clinic. Furthermore, the results obtained in the study show that the implemented IoMT system meets the security and sustainability requirements and has shown positive results in terms of response time, sensitivity, specificity, precision, accuracy, F-Score, positive predictive value, value predictive negative, false positive rate, false negative rate, and error rate.

In addition, it is highlighted that the IoMT system has achieved a high success rate in transmitting data from the devices to the cloud system and a high precision in the vital signs data collected by the monitoring devices. These results support the reliability and accuracy of the system in data collection and transmission. Patients' frequency of use of the system has also been noted as high, indicating positive acceptance and improvement in healthcare by allowing patients to monitor their health status in real time, even outside the clinic. Additionally, the contribution of this work is mentioned by analyzing and summarizing similar studies that evaluate the effectiveness of IoMT systems in healthcare settings. These studies demonstrate that IoMT systems detect health problems and patient follow-up in various medical contexts.

5. Conclusions

The results obtained in this study show that implementing an IoMT system in a medical clinic can improve patient care by allowing the monitoring of their vital signs in real-time and from anywhere. In addition, medical personnel achieved high accuracy in collecting vital signs data and a fast response time in case of system alerts. The frequency

of use of the system by patients was moderate, suggesting that patients may benefit from increased knowledge and understanding of the benefits of using the system.

However, limitations were also identified in this study, such as the lack of long-term data on the resolution rate of health problems detected by the system and the need for a more significant effort in educating patients on the use of the system. In addition, although a high success rate was obtained in the transmission of data from the devices to the cloud system, it is recommended to continue improving the devices' connectivity and the cloud platform's stability.

Regarding future work, it is suggested that a longitudinal study be carried out to evaluate the long-term effectiveness of the IoMT system in improving patient care and disease prevention. In addition, new data analysis techniques can be explored to improve the accuracy of detecting health problems. Improvements to the system interface can also be considered for a better user experience and greater acceptance of the system by patients. This study provides a solid foundation for implementing an IoMT system in a medical clinic and highlights its potential to improve patient care and prevent disease.

Author Contributions: Conceptualization, W.V.-C.; methodology, W.V.-C.; software, J.G.-O.; validation, I.U.-C.; formal analysis, W.V.-C.; investigation, J.G.-O.; data curation, W.V.-C. and I.U.-C.; writing—original draft preparation, W.V.-C.; writing—review and editing, J.G.-O.; visualization, J.G.-O.; and supervision, W.V.-C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: This research study uses data that have already been collected and anonymized so that participants cannot be identified; therefore, ethical review and approval are considered waived.

Informed Consent Statement: Written informed consent has been obtained from the patient(s) to publish this paper.

Data Availability Statement: The data can be sent to the interested parties, for which they must be communicated to the email of the corresponding author.

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

Appendix A

```
import androidx.appcompat.app.AppCompatActivity;
import android.os.Bundle;
import android.view.View;
import android.widget.Button;
import android.widget.EditText;
import android.widget.Toast;
public class MainActivity extends AppCompatActivity {
EditTextnombre, apellido, edad, direccion;
Buttonbtn_registrar;
@Override
protected void onCreate(Bundle savedInstanceState) {
super.onCreate(savedInstanceState);
setContentView(R.layout.activity_main);
nombre = findViewById(R.id.nombre);
apellido = findViewById(R.id.apellido);
edad = findViewById(R.id.edad);
direccion = findViewById(R.id.direccion);
btn_registrar = findViewById(R.id.btn_registrar);
btn_registrar.setOnClickListener(newView.OnClickListener(){
@Override
public void onClick(View v) {
```

```
String nombre_txt = nombre.getText().toString().trim();
String apellido_txt = apellido.getText().toString().trim();
String edad_txt = edad.getText().toString().trim();
String direccion_txt = direccion.getText().toString().trim();
if(nombre_txt.isEmpty()||apellido_txt.isEmpty()||edad_txt.isEmpty()||
direccion_txt.isEmpty()){
Toast.makeText(MainActivity.this,"Porfavor,completatodosloscampos",
Toast.LENGTH_SHORT).show();
} else {
Toast.makeText(MainActivity.this,"Registroexitoso",Toast.LENGTH_SHORT).show();
nombre.setText("");
apellido.setText("");
edad.setText("");
direccion.setText("");
}
}
});
```

References

1. Yaacoub, J.P.A.; Noura, M.; Noura, H.N.; Salman, O.; Yaacoub, E.; Couturier, R.; Chehab, A. Securing internet of medical things systems: Limitations, issues and recommendations. *Future Gener. Comput. Syst.* **2020**, *105*, 581–606. [CrossRef]
2. Syed, L.; Jabeen, S.; Manimala, S.; Alsaeedi, A. Smart healthcare framework for ambient assisted living using IoMT and big data analytics techniques. *Future Gener. Comput. Syst.* **2019**, *101*, 136–151. [CrossRef]
3. Shankar, N.; Nallakaruppan, M.K.; Ravindranath, V.; Senthilkumar, M.; Bhagavath, B.P. Smart IoMT Framework for Supporting UAV Systems with AI. *Electronics* **2023**, *12*, 86. [CrossRef]
4. Tarikere, S.; Donner, I.; Woods, D. Diagnosing a healthcare cybersecurity crisis: The impact of IoMT advancements and 5G. *Bus. Horizons* **2021**, *64*, 799–807. [CrossRef]
5. Basha, A.J.; Rajkumar, N.; Alzain, M.A.; Masud, M.; Abouhawwash, M. Fog-based Self-Sovereign Identity with RSA in Securing IoMT Data. *Intell. Autom. Soft Comput.* **2022**, *34*, 1693–1706. [CrossRef]
6. Ravikumar, G.; Venkatachalam, K.; Masud, M.; Abouhawwash, M. Cost Efficient Scheduling Using Smart Contract Cognizant Ethereum for IoMT. *Intell. Autom. Soft Comput.* **2022**, *33*, 865–877. [CrossRef]
7. Aldhyani, T.H.; Khan, M.A.; Almaiah, M.A.; Alnazzawi, N.; Hwaitat, A.K.A.; Elhag, A.; Shehab, R.T.; Alshebami, A.S. A Secure internet of medical things Framework for Breast Cancer Detection in Sustainable Smart Cities. *Electronics* **2023**, *12*, 858. [CrossRef]
8. Shakeel, T.; Habib, S.; Boulila, W.; Koubaa, A.; Javed, A.R.; Rizwan, M.; Gadekallu, T.R.; Sufiyan, M. A survey on COVID-19 impact in the healthcare domain: Worldwide market implementation, applications, security and privacy issues, challenges and future prospects. *Complex Intell. Syst.* **2023**, *9*, 1027–1058. [CrossRef]
9. Almaiah, M.A.; Hajjej, F.; Ali, A.; Pasha, M.F.; Almomani, O. A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS. *Sensors* **2022**, *22*, 1448. [CrossRef]
10. Ksibi, S.; Jaidi, F.; Bouhoula, A. A Comprehensive Study of Security and Cyber-Security Risk Management within e-Health Systems: Synthesis, Analysis and a Novel Quantified Approach. *Mob. Netw. Appl.* **2022**. [CrossRef]
11. Ahmed, J.; Nguyen, T.N.; Ali, B.; Javed, M.A.; Mirza, J. On the Physical Layer Security of Federated Learning Based IoMT Networks. *IEEE J. Biomed. Health Inform.* **2023**, *27*, 691–697. [CrossRef] [PubMed]
12. Sun, Y.; Lo, F.P.; Lo, B. Security and Privacy for the internet of medical things Enabled Healthcare Systems: A Survey. *IEEE Access* **2019**, *7*, 183339–183355. [CrossRef]
13. Srivastava, J.; Routray, S.; Ahmad, S.; Waris, M.M. Internet of medical things (IoMT)-Based Smart Healthcare System: Trends and Progress. *Comput. Intell. Neurosci.* **2022**, *2022*, 7218113. [CrossRef] [PubMed]
14. Toghuj, W.; Turab, N. A Survey on Security Threats in the internet of medical things (IoMT). *J. Theor. Appl. Inf. Technol.* **2022**, *100*, 3361–3371.
15. Wagan, S.A.; Koo, J.; Siddiqui, I.F.; Qureshi, N.M.F.; Attique, M.; Shin, D.R. A Fuzzy-Based Duo-Secure Multi-Modal Framework for IoMT Anomaly Detection. *J. King Saud Univ.-Comput. Inf. Sci.* **2023**, *35*, 131–144. [CrossRef]
16. Ali, A.; Almaiah, M.A.; Hajjej, F.; Pasha, M.F.; Fang, O.H.; Khan, R.; Teo, J.; Zakarya, M. An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. *Sensors* **2022**, *22*, 572. [CrossRef]
17. Almaiah, M.A.; Ali, A.; Hajjej, F.; Pasha, M.F.; Alohali, M.A. A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things. *Sensors* **2022**, *22*, 2112. [CrossRef] [PubMed]
18. Jain, S.; Nehra, M.; Kumar, R.; Dilbaghi, N.; Hu, T.Y.; Kumar, S.; Kaushik, A.; zhong Li, C. Internet of medical things (IoMT)-integrated biosensors for point-of-care testing of infectious diseases. *Biosens. Bioelectron.* **2021**, *179*, 113074. [CrossRef]
19. Wazid, M.; Das, A.K.; Rodrigues, J.J.; Shetty, S.; Park, Y. IoMT Malware Detection Approaches: Analysis and Research Challenges. *IEEE Access* **2019**, *7*, 182459–182476. [CrossRef]

20. Vaiyapuri, T.; Binbusayyis, A.; Varadarajan, V. Security, Privacy and Trust in IoMT Enabled Smart Healthcare System: A Systematic Review of Current and Future Trends. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 731–737. [CrossRef]
21. Hameed, S.S.; Hassan, W.H.; Latiff, L.A.; Ghabban, F. A systematic review of security and privacy issues in the internet of medical things; The role of machine learning approaches. *PeerJ Comput. Sci.* **2021**, *7*, e414. [CrossRef] [PubMed]
22. Dwivedi, R.; Mehrotra, D.; Chandra, S. Potential of internet of medical things (IoMT) applications in building a smart healthcare system: A systematic review. *J. Oral Biol. Craniofacial Res.* **2022**, *12*, 302–318. [CrossRef]
23. Al-Dhaen, F.; Hou, J.; Rana, N.P.; Weerakkody, V. Advancing the Understanding of the Role of Responsible AI in the Continued Use of IoMT in Healthcare. *Inf. Syst. Front.* **2021**. [CrossRef] [PubMed]
24. Kumar, R.; Tripathi, R. Towards design and implementation of security and privacy framework for internet of medical things (IoMT) by leveraging blockchain and IPFS technology. *J. Supercomput.* **2021**, *77*, 7916–7955. [CrossRef]
25. Almogren, A.; Mohiuddin, I.; Din, I.U.; Almajed, H.; Guizani, N. FTM-IoMT: Fuzzy-Based Trust Management for Preventing Sybil Attacks in internet of medical things. *IEEE Internet Things J.* **2021**, *8*, 7916–7955. [CrossRef]
26. Binbusayyis, A.; Alaskar, H.; Vaiyapuri, T.; Dinesh, M. An investigation and comparison of machine learning approaches for intrusion detection in IoMT network. *J. Supercomput.* **2022**, *78*, 17403–17422. [CrossRef]
27. Wazid, M.; Singh, J.; Das, A.K.; Shetty, S.; Khan, M.K.; Rodrigues, J.J. ASCP-IoMT: AI-Enabled Lightweight Secure Communication Protocol for internet of medical things. *IEEE Access* **2022**, *10*, 57990–58004. [CrossRef]
28. lakhan, A.; Mohammed, M.A.; Ibrahim, D.A.; Abdulkareem, K.H. Bio-inspired robotics enabled schemes in blockchain-fog-cloud assisted IoMT environment. *J. King Saud Univ.-Comput. Inf. Sci.* **2023**, *35*, 1–12. [CrossRef]
29. Papaioannou, M.; Karageorgou, M.; Mantas, G.; Sucasas, V.; Essop, I.; Rodriguez, J.; Lymberopoulos, D. A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT). *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4049. [CrossRef]
30. Ghubaish, A.; Salman, T.; Zolanvari, M.; Unal, D.; Al-Ali, A.; Jain, R. Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security. *IEEE Internet Things J.* **2021**, *8*, 8707–8718. [CrossRef]
31. Dilawar, N.; Rizwan, M.; Ahmad, F.; Akram, S. Blockchain: Securing internet of medical things (IoMT). *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 82–89. [CrossRef]
32. Jolfaei, A.A.; Aghili, S.F.; Singelee, D. A Survey on Blockchain-Based IoMT Systems: Towards Scalability. *IEEE Access* **2021**, *9*, 148948–148975. [CrossRef]
33. Khan, I.A.; Moustafa, N.; Razzak, I.; Tanveer, M.; Pi, D.; Pan, Y.; Ali, B.S. XSRU-IoMT: Explainable simple recurrent units for threat detection in internet of medical things networks. *Future Gener. Comput. Syst.* **2022**, *127*, 181–193. [CrossRef]
34. Talaminos-Barroso, A.; Reina-Tosina, J.; Roa, L.M. Adaptation and application of the IEEE 2413-2019 standard security mechanisms to IoMT systems. *Meas. Sens.* **2022**, *22*, 100375. [CrossRef]
35. Nayak, J.; Meher, S.K.; Souri, A.; Naik, B.; Vimal, S. Extreme learning machine and bayesian optimization-driven intelligent framework for IoMT cyber-attack detection. *J. Supercomput.* **2022**, *78*, 14866–14891. [CrossRef]
36. Almalki, J.; Shehri, W.A.; Mehmood, R.; Alsaif, K.; Alshahrani, S.M.; Jannah, N.; Khan, N.A. Enabling Blockchain with IoMT Devices for Healthcare. *Information* **2022**, *13*, 448. [CrossRef]
37. Garg, N.; Wazid, M.; Das, A.K.; Singh, D.P.; Rodrigues, J.J.; Park, Y. BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for internet of medical things Deployment. *IEEE Access* **2020**, *8*, 95956–95977. [CrossRef]
38. Khan, H.A.; Abdulla, R.; Selvaperumal, S.K.; Bathich, A. IoT based on secure personal healthcare using RFID technology and steganography. *Int. J. Electr. Comput. Eng.* **2021**, *11*, 3300–3309. [CrossRef]
39. Pelekoudas-Oikonomou, F.; Zachos, G.; Papaioannou, M.; de Ree, M.; Ribeiro, J.C.; Mantas, G.; Rodriguez, J. Blockchain-Based Security Mechanisms for IoMT Edge Networks in IoMT-Based Healthcare Monitoring Systems. *Sensors* **2022**, *22*, 2449. [CrossRef]