I.J. Wireless and Microwave Technologies, **2024, 6, 68-80**
Published Online on December 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2024.06.05

IoMT Survey: Device, Architecture, Communication Protocols, Application and Security

Dina Riyadh Ibrahim*
Electronics and communications engineering/electronics, University of Mosul, Iraq
Email: Dina.22enp21@student.uomosul.edu.iq
*Corresponding Author

Mohammed Younis Thanoun
Electrical engineering/ electronic and communication from the University of Mosul, Iraq
Email: myounisth@uomosul.edu.iq

Received: 12 July, 2024; Revised: 15 August, 2024; Accepted: 24 October, 2024; Published: 08 December, 2024

Abstract: The technology-based lifestyle has led to a rise in people suffering from obesity, which in turn has led to the emergence of many chronic diseases such as elevated blood sugar and blood pressure, this give researchers a good reasons to develop Internet of Things networks, as the entry of technical innovations has led to Artificial intelligence in the medical field has revolutionized the provision of medical services and facilitated the lives of patients, from monitoring blood sugar levels to using remote surgery techniques, as it has saved a lot of effort and money for both the doctor and the patient at the same time, but these advantages open a wide scope for many problems as well. This survey studied the medical Internet of Things network in terms of presenting the definition, structure, types of devices used, their applications, and some of the communication protocols used in it. The attacks that the medical Internet of Things network may be exposed to were also classified based on the concerns they cause, and the solutions proposed by the researchers were presented. On the other hand, the previous works of the researchers were classified according to the types of devices used, communication protocols, and network security. In each of the mentioned parts, what the researchers have done and their contributions in this field were discussed, analyzed, and a review of the proposed future works in the used literature was presented.

Index Terms: IoMT, wearable and implantable devices , Eavesdropping , Traffic analysis , Wi-fi , HECC , DES

1. Introduction

Internet of Things systems in the medical field are considered as a one of the most promising areas at the level of computer networks, not only because they are close to human health and able to influence and control large parts of areas of his life, but because they also use multiple technologies, starting with short-range Bluetooth. From monitoring blood sugar levels to using remote surgery techniques, which saved time, effort and money to perform remote surgeries that previously cost both the patient and the doctor a lot. The Internet of Medical Things is known as one of the applications of the Internet of Things in the medical field, which helps improve the quality of life of patients. It is a platform for exchanging sensitive information[1]. It also provides a link between IoT technologies and healthcare services with the aim of providing both real-time, remote and remote monitoring and treatment of patients[2]. It is an advanced model of the Internet of Things technology that aims to revolutionize the field of health care. It works to integrate the power of sensors with network technologies, and through it, data is collected and analyzed in real time[3]. With the use of an integrated network, IoT helps to enable real-time patient monitoring and the unification of all healthcare domains to function as a single entity. elevated standards of accuracy, trust, security, and privacy. IT and medical personnel should receive training to make sure they are not attacked [4].

2. Internet of Medical Thinks

2.1 Application

IoMT technologies are developing quickly, and as a result, they are being used in a variety of healthcare settings to enhance monitoring, diagnosis, and therapy. An overview of the IoMT's promising uses in several fields is given in this section.

A. Remote Patient Monitoring:

The Internet of Medical Things has provided many advantages in terms of providing health care to patients inside the hospital, in addition to the ability to monitor patients remotely and take vital signs such as temperature, pulse, and pressure. Thus, the patient is no longer forced to travel and reach the hospital for the purpose of conducting examinations, as this has become In recent years, this has become common and available in most countries, and with the increasing medical development, more accurate and useful techniques have emerged for the patient in terms of monitoring the patient remotely. These are remote surgical operations, which are classified into: Analog surgery Remote diagnosis [5]

B. Digital biomarker

The process of monitoring a person's vital signs, which can be used to analyze the patient's condition and classify its degree of severity, is one of the most important stages of studying the patient's condition and deciding the appropriate treatment[5].

- Glucose Level Monitoring:

The traditional method of measuring blood sugar levels in patients is no longer useful due to fluctuations in sugar levels that the traditional process may not detect. Therefore, it was proposed to check the glucose level automatically and continuously[6].

- Temperature Monitoring

Tracking the patient's temperature change helps doctors infer the health status of many diseases, as traditional methods of measuring temperature have become uncomfortable for the patient or may cause infection to be transmitted, Authers in [7] proposed that ear students could be worn to track the temperature change using infrared rays[7].

C. Heart disease:

Using the Internet of Medical Things to examine heart disease allows individuals to perform self-examinations for early detection of heart disease, and it is one of the most important first steps in diagnosing heart disease[7].

- Heart Rate Monitoring

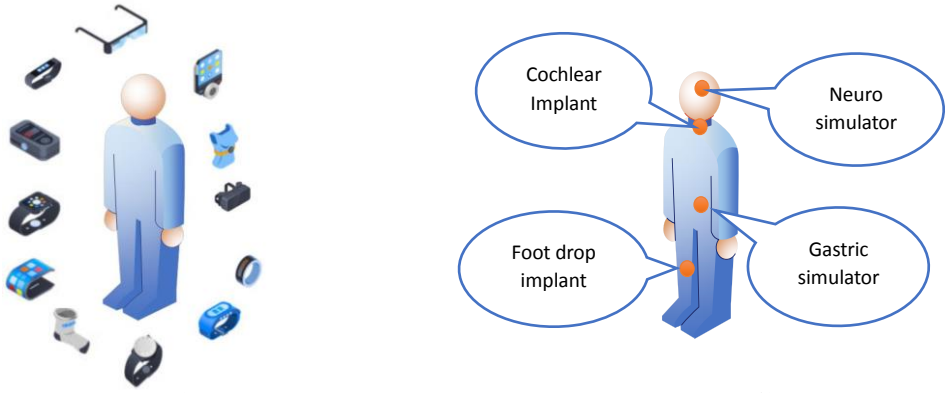
The process of measuring heart rate in a hospital is more complicated than measuring glucose because it requires connecting the patient to the device via wires that restrict his movement. Internet of Things devices provide a reliable way to monitor heart rate[6]

- Blood Pressure Monitoring

Measuring blood pressure is one of the most important diagnostic procedures. The development of the Internet of Medical Things and its integration with sensors has led to the possibility of monitoring blood pressure remotely. Authors in [7] proposed a wearable device that works to measure diastolic blood pressure and systolic and store the result in the cloud [7]

2.2 Devices in IoMT

Implantable sensors are a promising technology that offers many advantages in the field of health care. Such as treating a specific medical condition, monitoring and improving the performance of a part of the body, or providing the patient with certain abilities. After integrating communication protocols with artificial intelligence with this (Implantable sensors) type of device, it gave patients more independence while reducing costs and the possibility of remote monitoring. Fig 1. show smart biomedical wearable implantable measurement devices[8].



(a) (b)

Fig. 1. Intelligent biomedical measuring instruments, (a) intelligent wearable measuring instruments (b) intelligent implanted measurement tools [8].

Table 1. provides a simple definition of the difference between wearable devices versus implantable devices in terms of application space, benefits and drawbacks in an IoT healthcare network.

Table 1. Types of IoMT devices.

Type	Application Area	Advantages	Disadvantages
Internet of wearable devices (IWD)	Remote Patient Monitoring Chronic Disease Management Fitness Tracking	Monitoring patients in non-critical cases	Limited battery life Concerns about the accuracy and reliability The potential for data breaches and cyber-attacks
Implantable medical devices (IMD)	Chronic Disease Management, Patient Monitoring	low-power consumption small storage space small batteries very long battery life	Concerns about the security and privacy the risks associated with surgical implantation
Ref	[5], [9]		

2.3 Communication Protocols

Continuous monitoring of an individual's health with the aim of early diagnosis of diseases is one of the most important applications of the Internet of Medical Things. Therefore, transmission delay is a major problem that the network suffers from and directly affects decision-making related to patients' health, as uplink transmission in the OFDMA system can cause an unacceptable delay for the sensors due to Due to its random nature. Based on the above, a scheduling program was proposed that complies with the requirements of access time using the wireless fidelity (Wi-Fi) standard IEEE 802.11be. It works to allocate UL (uplink) channel resources and take into account the access and movement class [10] . Communications protocols provide interaction between medical devices such as sensors and monitoring devices close to the patient (in the perception layer or sensor layer), shown in Figures (1) and (2). These protocols work to mine data up to the network layer, which in turn works using its protocols transform data into a format suitable for the medical application in question, reaching the application layer to provide appropriate treatment for the patient Authors in [2] classified communication protocols based on the layer in which they operate [2] , while Authors in [12] classified communications protocols according to the medical devices that use them [12].

Table 2. shows the characteristics of some standards in terms of frequency, range, error rate, and encryption algorithms for each technology.

Table 2. Communication technologies characteristics.

technology	Standard	Layer	Device	Frequency	Transmission range	Bitrate	Encryption
Bluetooth	802.15.1	PHY	IWD - IMD	13.56 MHz, 2.4 GHz ISM	10 to 30m	2.1 Mbit/s	Shared key
Zigbee	802.15.4	PHY	IWD-IMD	8 MHz, 915 MHz, 2.4 GHz	10 to 20 m	250 Kbit/s	AES - CBC−MAC
IEEE 802.15.6	802.15.6	Net	IWD-IMD	HBC, UWB, NB	< 100m	75.9 Kbit/s to 15.6 Mbit/s	AES− CCM
Wi-fi	802.11	Net	IWD	2.4 GHz	100m	54 Mbit/s	WPA2
Ref	[11, 12, 13]						

Due to the increasing diversity in the medical Internet of Things network, which in turn imposes many complexities on the network, it is not possible to use a single protocol in communications for all types of devices, as the

nature of the devices and their ability to process and communicate differ from small wearable or implantable devices to a complete health system such as hospitals[2].

Based on the above, Table 3. shows classifications of device types, from display devices to processing devices and devices specific to the hospital system, with the protocols used in each of these classifications.

Table 3. IoMT Devices classifications and its communication protocols.

Categories	Type	Device	Protocol
Physiologic Monitoring Devices	Wearable Monitoring Medical Device	Electroencephalogram (EEG)	Z-Wave- Bluetooth - ZigBee
		electrocardiogram (ECG),	
		electromyography (EMG),	
		blood pressure measuring	MQTT - HTTP
		Respiratory rate sensors	
		Body temperature	
	Ingestible Monitoring Medical Devices	pulse sensor	RFID- Bluetooth -WiFi
		the sensitive temperature sensor	
Medical Treatment Devices	Implantable Medical Devices	Implantable Cardioverter Defibrillators (ICDs)	NFC - RFID- ZigBee
		Cardiac Rhythmic Management (CRM)	
	Infusion Pump	Patient-controlled analgesia	
. In-Hospital Connected Medical Device	Institutional Medical Devices	Magnetic Resonance Imaging (MRI)	
		X-rays	
		Surgical Robotics.	
	In-hospital Medical Robotics	Surgical robotic	IrDA, RFID , Bluetooth , HTTP
		smart medical capsules,	
		Prosthetics	
		robot-assisted mental	
		social therapy	
		robotised patient monitoring systems	
Ref	[14], [15], [4]		

2.4 Architecture:

Since most communications protocols were not originally designed to meet the needs of medical devices, we therefore classify communications protocols and describe their main characteristics at the perception, network, and applications layer for medical devices, study the security characteristics and restrictions imposed on the protocols, and identify available mitigation controls[2] .There are many proposals available that explain the architecture of the Internet of Medical Things, of which two types are presented

Architecture 1: Chander Prabha and Aashim Garg propose to arrange the network structure based on its contents, as shown in Fig 1. which consists of [3] :

Sensor layer :which includes gadgets like smart watches and patient monitoring systems that interact with users directly, gather data, and transmit it to the next layer.

Fog layer: It consists of servers that work to redirect data to the cloud layer, in addition to its work in managing the safety and security of the system.

Cloud layer: It analyzes data, makes decisions, and helps store data for further analysis in the future[2]

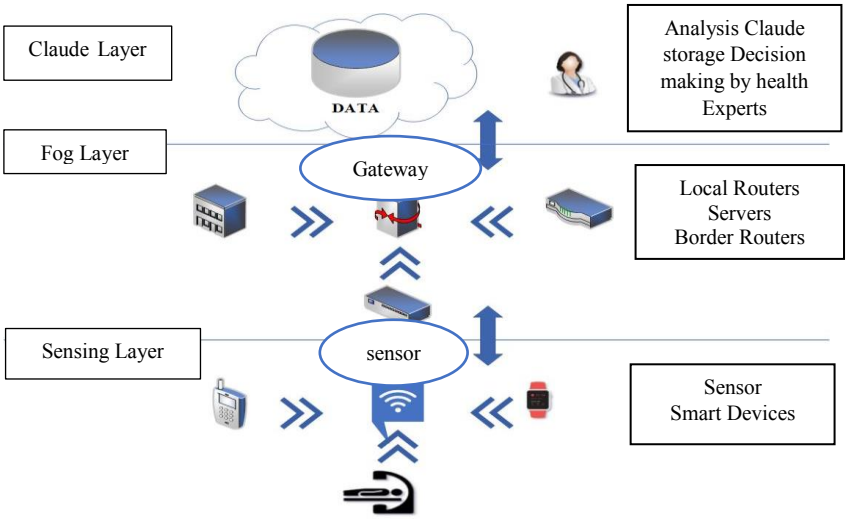


Fig. 2. Architecture of the IoMT-1(based on its contents)

Architecture 2: Sangeetha C P , Swathi Shabu , Althaf Ashraf [3] present other suggestion based on the function of the layers, as in the Fig 2.

Perception layer: This layer is located at the bottom of the network structure and is responsible for collecting information and extracting data

Network layer: The middle layer is responsible for data transfer services and consists of two sublayers, service and transfer

Application layer: It is the upper layer that uses the information received from the network layer to maintain medical data and make decisions related to it.[3]

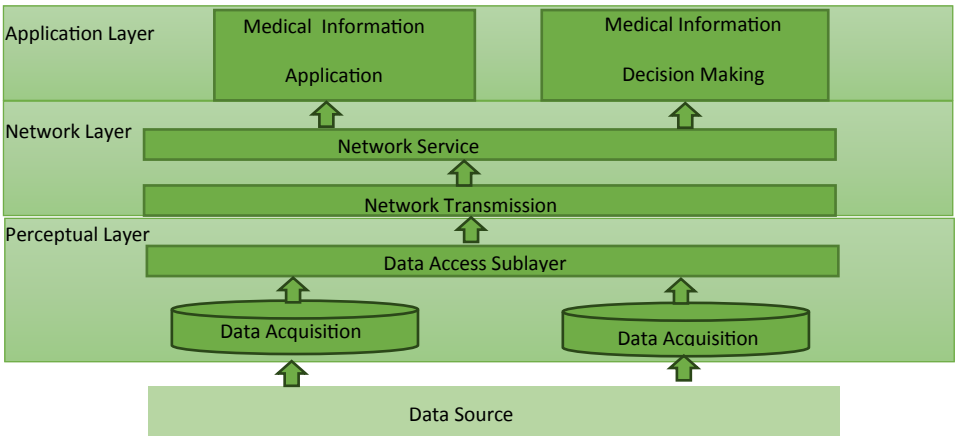


Fig. 3. Architecture of the IoMT-2(based on the function of the layers)

3. Security Aspect

Medical devices available on the Internet provide health care providers with many services, such as managing diseases and medications, improving food supplies, and reducing costs. For these reasons, the health care devices market sector, which includes the Internet, including what is known as the medical Internet, is a market that has growth in recent years, and its profits are expected to increase to millions of dollars. With all this diversity and the services provided, it has opened the way for new types of attacks, the causes of which can be investigated:

1) Sharing sensitive patient data
2) Due to the large number of devices in the network, problems of heterogeneity and compatibility appear
3) Security problems related to integrity, confidentiality, and availability
4) Because this type of network uses wireless communication, it makes it more vulnerable to violations
5) The network needs applications in terms of operation, monitoring and control, which provides an environment for attackers to violate authentication, authorization and security.
6) Due to the limited capabilities of the sensors, many of which lack encryption, they become exposed to attackers[16]

Confidentiality requirements are classified into two categories.

The first: confidentiality requirements within a single network, which are:

1) It is necessary to verify network users to prevent the injection of false data by attackers
2) The necessity of encrypting data during transmission to avoid spam attacks and disclosure of data to unauthorized persons
3) Avoid system failure and provide security and integrity in data transmission against information tampering attacks
4) Providing medical service and disclosing data to prevent denial or denial of service by attackers.

Second: Confidentiality requirements between the network and the outside world include:

1) Encrypt data during transmission to avoid modification and privacy disclosure
2) Determine user privileges, access, and control policy
3) Do not deny the message[17].

Table 4. shows a classification of the concerns facing the Internet of Things, the attacks it is exposed to, and their causes, in order to prepare for presenting what has been studied in this field, the contributions of researchers, and the proposed solutions to these concerns.

Table 4. IoMT security aspect attacks reason and solution.

Security aspect	Attacks	reason
Confidentiality	Eavesdropping [12]	Messages are broadcast across wireless channels. unencrypted line of communication
	Data interception[18]	Insecure Channels Accessible Wireless Transmission
	Packet capturing[19]	Accessible Wireless Transmission Channels That Are Not Secure Are Not Encrypted
Privacy	Traffic analysis [19]	Information about the source and destination is not encrypted. Absence of safe routes .Inadequate encryption technique
	Identity/Location track in [19]	Insufficiently safe channels Parameters for identification and location are not encrypted.
integrity and authentication	Message Tampering-Alteration[20]	Lack of a source authentication and data integrity protection system
	Malicious data injection [20]	
	Cloning & Spoofing[21]	
Availability	Jamming [23]	targets WiFi IoMT devices or access points
	Denial Of Service	Lack of Backup Devices
	Distributed Denial of Service (DDOS)[22]	Exploiting devices turning them into bots
	Flood[20]	Overloads and Depletes IoMT's Resources with False Injection of Information
	Delay	Overwhelms & Prevent or Severely Delays any Transceiving of Medical Information
Authentication	Man-in-the-Middle [18]	Poor authentication scheme (one factor)
	Replay [23]	Weakness in the authentication protocol
	Brute force[22]	Weak password one authentication factor
	Session Hijacking [23]	Lack of/Poor Encryption Non-Secure Channels

3.1 Devices in IoMT related work

Implantable sensors are a promising technology that offers many advantages in the field of health care. Such as treating a specific medical condition, monitoring and improving the performance of a part of the body, or providing the patient with certain abilities. After integrating communication protocols with artificial intelligence with this type of device, it gave patients more independence while reducing costs and the possibility of remote monitoring.

Authors in [4] present security techniques for IoT systems and study the issues of security protocols, privacy, and interoperability between systems with the aim of reducing costs, improving patient monitoring, and enhancing personalized healthcare, reviewing implantable or wearable sensors and their investments in telesurgery, studying the security challenges and threats, studying the reasons, and providing appropriate solutions for each of them in terms of encryption types and algorithms. The integration of ECC with the RSA algorithm was approved once the CHF hash function was integrated with ECC, as this integration process ensures confidentiality, security, reduces complexity, and solves the problem of sharing keys with the wallet. About data privacy and accessibility. Given the sensitivity and privacy of medical information transmitted over the IoT network, it has become necessary to take security measures to secure the transmission, collection, and storage of data, as three encryption algorithms were studied: symmetric, asymmetric, and keyless, and their impact on the network.[4].

Data integration in the medical Internet of Things network is one of the most important challenges facing the network due to the diversity of data sources such as merging imaging scans and laboratory results, which provides a clearer picture of the patient's condition and helps the doctor in more accurate diagnosis and determining the appropriate treatment. The process of collecting data from sensors in the medical Internet of Things network has many implications due to its importance, quality and large quantity, and may affect the accuracy of diagnosis and decision-making. In this research, an algorithm was studied to detect epileptic seizures within the Internet of Things network, which means the presence of anything suspicious in the network with an accuracy ranging between. The biggest challenge remains improving the stages of data collection, protection and storage, in addition to unifying data coming from multiple sources in order to facilitate its integration and analysis. A group of fields in which data from sensors was integrated were also presented, such as detecting epileptic seizures, remote surgery, detecting Alzheimer's disease remotely and digital biometrics. The Naive Bayes (ESDNB) algorithm, based on detecting epileptic seizures, has shown its effectiveness in collecting data. However, despite its high efficiency, it requires security measures to detect threats and malware. This study relies on encryption and blockchain technology to provide security to the system.[5].

Ensuring fair access to smart healthcare systems is one of the challenges facing the security of devices connected to the Internet of Medical Things network. Therefore, authors in [9] studied smart healthcare systems within the framework of the Internet of Medical Things and (5.0) features of healthcare, focusing on addressing the security of devices connected to this network and studying the services, applications and challenges they face. Data was also analyzed within the Internet of Medical Things environment using artificial intelligence algorithms, deep learning and machine learning, to address weaknesses and ensure security in these systems.[9]A distributed network was designed by authors in [15] Wen and data compression techniques, scheduling algorithms, and data collection and redirection from sensors via tracking nodes were studied for the purpose of tracking the network and increasing the operating efficiency. The results of the proposed algorithm (weighted fair queueing) showed its superiority in terms of reducing the delay and jitter rate by 40% and 19.7% compared to the algorithm (Low Latency Queueing) and its effectiveness in terms of energy consumption compared to the direct path approach, in addition to improving applications related to the body regions network for self-organizing monitoring of population health.[15]Although wearable devices save the patient the risk of surgical operations and are more flexible than implantable devices, the remaining challenges remain on the ground. For the purpose of providing the process of collecting, transferring, and storing data in a secure manner, authors in [16] present the latest technologies for securing IoMT system data against physical and network attacks, and proposes a security framework that combines many security techniques, while clarifying the appropriate solutions for each attack Despite these many advantages, it entails many risks, the most important of which is endangering the patient's safety. The ease of access to data by hackers leads to a violation of privacy because these devices store sensitive information about the patient[16] .A scenario of healthcare network infrastructure was studied by authors in [18] with key stakeholders and cybersecurity requirements affecting the medical domain and threats were listed and linked to a framework (MITRE ATT&CK) to provide compatibility and interoperability for comparison purposes with previous works and provide countermeasures for each technology. The study also highlighted the cybersecurity challenges such as access control, trust management, security mechanisms and telehealth.[18]

Table 5. shows a summary of the problems studied in the literature on the devices used in the Internet of Medical Things described above, along with the proposed solutions and simulation methods used in each of them.

Table 5. Summary of previous work of the devices in IoMT.

Ref	problem	Solution	Simulation
[4]	Apply the essential security measures and IoT basics that allow various internal and external healthcare business areas to be connected. Solutions for protecting Internet of Things networks from data transmission, storage, and collecting threats. Examines how to make IoT more secure and sustainable by looking at the diverse security requirements, design issues that are inherent, and variety of security technologies.	ECC merges with RSA algorithm Once the CHF hash function is merged with ECC, this merge process ensures confidentiality and security, reduces complexity and solves the problem of sharing keys with the wallet Encryption Algorithms Symmetric Keys Asymmetric Keys and Keyless	Review
[5]	Integrating data into the IoT network is one of the most important challenges facing the network due to the diversity of data sources.	Epileptic seizures within the Internet of Things network	Review
[15]	distributed network was designed and data compression techniques, scheduling algorithms, and data collection and redirection from sensors via tracking nodes	weighted fair queueing	Implementation and Performance Evaluation
[16]	Providing secure data collection, transmission and storage	Techniques for securing medical IoT data against physical and network attacks , and a security framework is proposed that combines several security techniques.	Review
[18]	Access control, trust management, security mechanisms, and remote healthcare	key stakeholders and cybersecurity requirements affecting the medical domain and threats were listed and linked to a framework (MITRE ATT&CK) to provide compatibility and interoperability for comparison purposes with previous works and provide countermeasures for each technology	Review

3.2 Communication Protocols Related work:

The entry of technical innovations and medical devices into the field of health care has brought about a radical transformation in the field of service provision and availability, in exchange for increased security concerns. In order to clarify these concerns authors in [11] studied the security vulnerabilities in these devices, security tests, and attacks to which they may be exposed, such as tampering, espionage, and unauthorized access. The declarant also highlighted the weaknesses and measures available to address them[11] . The low-power IEEE 802.15.4 standard was used by authors in [13] in the construction of the wireless body area network. The impacts of a number of network features, including packet sizes, arrival times, and node counts, on connection dependability were investigated. The findings demonstrated that one of the key determinants of connection reliability is the packet delivery ratio. The network's ability to transmit data is impacted by the diversity of the testing environment. Our findings also demonstrate that, in order to obtain more than 90% PDR for every testing scenario, the optimal network dependability should be adjusted at more than 15 ms in the packet interval time [13]. The IEEW802.15.4e standard was used by authors in [24] to design a wireless sensor network using the low latency deterministic network (LLDN) super frame contained in this standard. Based on it, a new channel access mechanism was proposed and an analysis model was designed based on which the performance analysis of the proposed model was studied in terms of energy consumption, throughput, delay, and reliability of data transfer. The simulation results of the proposed network were compared with the analytical results, which showed a great match between the two. The IEEE 802.15.4 MAC mechanism was also used and compared with the proposed model to show its superiority in terms of reliability, throughput, and energy consumption[24]. A wireless sensor network is designed by authors in [25] using MAC protocol with an improved version of CSMA it that detects weak signals WSD. The proposed protocol increases throughput by reducing loss. The simulation was done using a simulation program (OMNet++) and a framework (MiXiM). Based on the simulation results, the proposed protocol (CSMA/WSD) provides higher throughput under increased error rates and distance between nodes with a significant decrease in average delay [25]. Table 6. shows a summary of the problems studied in the literature on the communication protocols used in the Internet of Medical Things described above, along with the proposed solutions and simulation methods used in each of them.

Table 6. Summary of previous work of the communication protocols in IoMT.

.ref	Problem	Solution	Simulation
[11]	tampering, espionage, and unauthorized access	studied the security vulnerabilities in these devices, security tests, and attacks to which they may be exposed	Survey
[13]	The IEEE 802.15.4 low power standard was used to build the wireless body area network. The effects of a number of network features, including packet sizes, access times, and number of nodes, on the reliability of the connection were investigated.	One of the key factors that determines the reliability of a connection is the packet delivery ratio. In order to get more than 90% PDR for each test scenario, the optimal network reliability should be set at more than 15 ms in packet interval time.	Implementation and experimental
[24]	Power consumption, throughput, latency and data transfer reliability	Using the IEEW802.15.4e standard to design a wireless sensor network using the low latency deterministic network (LLDN)	OMNeT++
[25]	improved version of CSMA it that detects weak signals WSD. increases throughput by reducing loss.	the proposed protocol (CSMA/WSD) provides higher throughput under increased error rates and distance between nodes with a significant decrease in average delay	OMNet++ MiXiM

3.3 Security Issues Related work:

To determine how the security is improved for transferring patient healthcare data, authors in [12] examined different existing techniques . Based on key characteristics, the data security protocols using AES, ECC, SHA-1, and hybrid encryption are examined. The most suitable approaches are evaluated after considering several data security methodologies for WBAN. Additionally, we examine the security in light of several attack scenarios [12].

To obtain a secure transfer process and provide confidentiality to the health system, authors in [17] proposed an idea to integrate the security of textual data with the medical image by integrating 2D-DWT-1L and 2D-DWT-2L technology with an encryption system using a combination of (AES) and (RSA) algorithms to begin with. Encryption and then hiding the result in the overlaid image. This technology provides concealment of the patient's confidential data and ensures minimal distortion of the transmitted image[17].

Authors in [26] pproposed a secure authentication system based on the hash chain, conducting a formal security analysis using the ROR model and an informal one, and validating the analysis using ProVerif. Simulation and comparison results show that the proposed lightweight system provides security features that support WBANs[26].

WBAN is primarily made up of implanted or wearable smart medical sensors and personal servers (as gateways) for remote monitoring of the body's vital processes and the ambient conditions around it. A medical sensor node (SN), personal server (PS), and medical server (MS)/cloud service (MCS) platform make up a typical medical WBAN application scenario. Authors in [27] proposed a lightweight and continuous authentication plan by creating a signal called Biokey to overcome the problem of impersonation and using a technique to reduce energy consumption and save time by reducing complex calculations and verifying the protocol to ensure mutual authentication between the personal PS node and the server node. The scheme provides security. Against attacks such as replay, impersonation, capture attack, data integrity and reducing the communication burden between the personal node and the server[27]. Authors in [28] using an IoMT system even when they were outside of the clinic. Positive findings proved that the implemented IoMT system complied with set security and sustainability standards. The real-time monitoring of the patients' vital signs, which enhanced the standard of care and enabled the early identification of potential problems, is one of the case study's significant statistical findings. Medical gadgets that have proven to be secure, long-lasting, and low-maintenance include the electrocardiograph, pulse oximeter, and blood pressure monitor. These findings were in line with earlier studies that had demonstrated the advantages of IoMT in terms of remote monitoring, the early identification of health issues, and improved medical decision-making[28]. WBAN works on the interaction of sensors through an open wireless channel, which makes it vulnerable to various threats. In addition to its work in monitoring data collection, it is a heterogeneous system. The sender and recipient can use different encryption algorithms. Based on the above authors in [29] proposed a heterogeneous authentication system using certificate-less encryption. On the sender side and identity-based encryption on the recipient side using the HECC scheme, which provides a security level similar to the ECC scheme, but with a more efficient approach and a smaller key size. The proposed scheme meets security and privacy and enhances efficiency in terms of calculations and communications [29]. Due to the widespread use of the Internet with a local infrastructure that may be weak in many cases, this leads to the emergence of security gaps and weak points at the ends of the network that target parts of the network such as default passwords and firmware. This has become a weapon against networks and the services they provide and for To mitigate this type of problem, authors in [30] made efforts to develop an intrusion detection system. This was done by using the signature and updating it in order to increase reliability. The ability of the proposal was enhanced and its performance was evaluated by creating signatures assigned to two of the most famous signature-based intrusion system identifiers with the ISOT, IoT23, and BoTIoT datasets, on the one hand, by detecting Anomalous traffic in terms of detection rates, number of alerts, detection time as well as peak CPU and memory usage[30].

Authors in [31] proposed to design a wireless network architecture (SD WBAN) with a light encryption system and the use of the HECC scheme to provide security for patient data. The proposed system has been divided using the MCDM approach based on the distance from the intermediate solution EDAS. The proposed system has proven its superiority in terms of communication, storage and computation costs[31]. A protocol was proposed that addresses attacks (offline password guessing, stolen smart card attacks, impersonation, and user anonymity) and then the ROM model was used to conduct a formal security analysis of the proposed protocol, which proved to provide efficiency, strength, and security in terms of costs for accounts and communications. Fast and easy access to the e-health cloud is a double-edged sword because it exposes data to new challenges such as integrity, security, and confidentiality. For authentication, factors such as smart card, password, and biometrics are used. Many ECC-based protocols have been introduced, but they It still suffers from security flaws and high costs. Authors in [32] introduced a protocol for the e-health cloud to thwart attacks such as password guessing, impersonation, and hiding the user's identity. The protocol was evaluated through formal security analysis using the Oracle random model[32].

In order to obtain the legitimacy of both the patient and the doctor, the anonymous authentication technology contributes to this without revealing privacy. However, the size of the key used in the encryption algorithms (DES, AES) and the process of sharing it remain among the problems that reduce the level of security in this technology. Therefore authors in [33] proposed a technology encryption with a smaller key size and the use of security analysis have proven its strength against potential attacks in terms of both storage, communication and computation costs[33]. After a wide range of ECG monitoring systems and health care for heart diseases, to increase the distinctiveness of the signal and ensure the speed of its transmission, it is necessary to choose a more effective method for encryption, ECG signal monitoring systems are sensitive systems and applications that require speed, stability, and accuracy in signal transmission. For this reason authors in [34] studied the DES and ECC encryption standards and compared the performance of each in effectively protecting data integrity. However, the results show that the former is superior in terms of speed, so it is recommended to use it in encryption in these systems in particular.[34]. Table 7. shows a summary of the literature on the security concerns studied and the problems and proposed solutions.

Table 7. Summary of previous work of the security concerns in IoMT.

Ref	Problem	Solution	Simulation
[12]	How to improve security for patient healthcare data transfer	Check data security protocols using AES, ECC, SHA-1 and hybrid encryption	
[17]	Safe transfer process and confidentiality of the health system	To integrate the security of text data with medical image by combining 2D-DWT-1L and 2D-DWT-2L technology with an encryption system using a combination of (AES) and (RSA) algorithms at first. Encryption and then hiding the result in the overlay image. This technology provides concealment of patient confidential data and ensures minimal distortion of the transmitted image	MATLAB R2015a
[26]	Secure Authentication System	Formal and informal security analysis using ROR model	ProVerif
[27]	Identity theft and use technology to reduce energy consumption and save time by reducing complex calculations.	Lightweight, continuous authentication plan	Performance evaluation
[28]	Track patients' vital signs	By enabling real-time and remote monitoring of vital signs, the installation of a medical IoT system at a clinic can enhance patient care.	statistical Implementation
[29]	Open wireless channel Heterogeneous system	Heterogeneous authentication scheme using certificate-less encryption on the sender side and identity-based encryption on the receiver side using the HECC scheme.	Analysis
[30]	Security vulnerabilities and weaknesses appear at the network edges targeting parts of the network such as default passwords and firmware.	Intrusion detection system. This is done using signature and updated for increased reliability.	Experimental
[31]	. To provide security for patient data.	A wireless network (SD WBAN) architecture with lightweight encryption and HECC scheme, the proposed system partitioning using MCDM approach based on distance from EDAS intermediate solution.	Performance Analysis
[32]	Offline password guessing, stolen smart card attacks, impersonation, user anonymity	An eHealth Cloud Protocol to Thwart Attacks	Formal security analysis using the random Oracle model
[33]	Anonymous Authentication Technology Key Size Used in Encryption Algorithms (DES, AES) and Sharing Process	تقنية تشWith a smaller key size and the use of security analysis, it has proven robust against potential attacks in terms of storage, communication and computing costs.	Analysis
[34]	Speed, stability and accuracy of ECG signal transmission	DES and ECC encryption	Analysis

4. Review Analysis

When analyzing what has been studied in terms of devices and protocols in the medical Internet of Things network, we notice that it consists of a diverse group of devices as shown in Table (3) in contrast to a large and diverse number of protocols in which each of these devices operates. This diversity has led to the creation of a heterogeneous environment due to the difference in data sources between images and laboratory results. The process of integrating data coming from different sources is one of the first challenges facing work in the field of the medical Internet of Things network. We face another challenge that lies in preserving this data when it is transferred through the network, while continuing to examine and study the weaknesses, concerns and attacks facing the network shown in Table (4) on the other hand, and providing ways to detect and protect problems. Therefore, integrating encryption algorithms enhances security, and artificial intelligence provides one of the promising methods in studying and analyzing the elements affecting network performance, such as the delay ratio, jitter, packet size, arrival time, number of nodes, belt delivery ratio, packet interval, and energy consumption, as these elements affect reliability. Network performance.

5. Proposed Solution and Future Directions

1. To lower the cost of installing visual monitoring via the Internet of Things, look into the possibility of upgrading these devices when connected to the network. [4] .
2. Develop continuing countermeasures for malware that infects networks [4].
3. Create ongoing strategies to combat network-based malware.[5]
4. Enhancing the phases of data gathering, security, and archiving; also, consolidating data from disparate sources to ease integration and analysis[5].
5. Technological advancements for the Internet of Medical Things and addressing issues with infrastructure expenses, regulatory compliance, standardization, stress on the network now in use, security, and privacy in the healthcare system [9].
6. AI algorithms (deep learning or machine learning) are being used to promote a paradigm shift in data analytics inside a data-driven environment in order to solve vulnerabilities and maintain security in smart healthcare systems. By combining next-generation IoT technologies with 5G and 6G networks, internet connection will be improved and network load will be reduced [9].
7. The method can assist in configuring the basic CSMA/CA parameters for WBANs applications without necessitating the development of a new protocol and improve data communication throughput by preventing network retransmissions and data collisions. [13].
8. In order to improve system effectiveness, data security issues in data processing must be addressed. Important physiological signal data must also be further integrated with the relationship between injury location and severity to create a more thorough priority scheme. Stress and data collection must be balanced. Applications for group health monitoring could include fall detection systems, disaster rescue operations, and crowd control for a hiking group[15].
9. The concept can be used in WSNs for a variety of applications, including automated dispensing, factory automation, fall detection systems, fire detection and alarm systems, robotics, airport logistics, and many more emerging automated applications.[24].
10. Upgrading the fundamental CSMA MAC protocol for use in critical situations begins with the creation of the new CSMA/WSD protocol. [25].
11. To assess the IoT system's long-term efficacy in enhancing patient care and reducing disease, conduct a longitudinal study [28].
12. It is possible to investigate new methods of data analysis to increase the precision of health problem detection [28].
13. Think about enhancing the system's user interface to enhance patient acceptance of the system and enhance user experience[28].
14. Provide a new asymmetric authentication system in which the private key and partial private key can be sent to users by the key generation center via an open channel without being seen by attackers. [29]
15. Use the available labeled datasets to train the anomaly detection module after evaluating the efficiency in terms of accuracy, F-measure, and FAR, for use in anomaly detection as well as automated signature generation process [30] .
16. Creating a sophisticated WBAN communication protocol to employ various queuing algorithms, including weighted fairness and priority queuing, to enhance Quality of Service (QoS) [31].
17. Utilizing 5G communication technology in conjunction with fog/edge-based signal-assisted cryptography and quantum cryptography to increase security and privacy at a reduced cost [31].
18. Maintaining the privacy of WBAN users' location as they access the WBAN network from different locations as they travel from one place to another [33].
19. With the capacity to combine the two algorithms, analyze a sizable volume of data, and execute encryption and decryption in real time.[34]

6. Conclusion

In spite of the fact that the Internet of Medical Things makes it easier for patients and doctors to communicate, lowers patient health care costs, and grants patients greater mobility and independence with the option of ongoing remote monitoring, this advancement has left sensor networks vulnerable to a variety of threats. It has become remotely accessible to hackers and others with access, which carries a number of concerns, the most significant of which is jeopardizing patient safety while breaching the confidentiality of sensitive patient data on the network. The process of combining the ECC and HECC algorithms with encryption algorithms like RSA, DES, AES, and SHA-1, as well as mixed encryption with support for communications protocols using artificial intelligence algorithms Neural Network and its derivatives and Fuzzy Logic, is one of the solutions based on the security measures that were presented suggested to improve the healthcare network's security and privacy.

References

[1] F. Kamalov, B. Pourghebleh, M. Gheisari, Y. Liu, and S. Moussa, "Internet of Medical Things Privacy and Security: Challenges, Solutions, and Future Trends from a New Perspective," Feb. 01, 2023, MDPI. doi: 10.3390/su15043317.

[2] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, "Security in iomt communications: A survey," Sep. 01, 2020, MDPI AG. doi: 10.3390/s20174828.

[3] S. C. P, S. Shabu, and A. Ashraf, "Internet of Medical Things: Architecture, Applications and Challenges," Journal of Informatics Electrical and Electronics Engineering, vol. 04, no. 101, pp. 1–10, 2023, doi: 10.54060/jieee.202.

[4] B. Bhushan, A. Kumar, A. K. Agarwal, A. Kumar, P. Bhattacharya, and A. Kumar, "Towards a Secure and Sustainable Internet of Medical Things (IoMT): Requirements, Design Challenges, Security Techniques, and Future Trends," Apr. 01, 2023, MDPI. doi: 10.3390/su15076177.

[5] S. F. Ahmed, M. S. Bin Alam, S. Afrin, S. J. Rafa, N. Rafa, and A. H. Gandomi, "Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions," Information Fusion, vol. 102, Feb. 2024, doi: 10.1016/j.inffus.2023.102060.

[6] N. Venu, K. Kumar Vaigandla, and A. Arunkumar, "Investigation on Internet of Things(IoT) : Technologies, Challenges and Applications in Healthcare," 2022. [Online]. Available: https://www.researchgate.net/publication/361923382

[7] B. Pradhan, S. Bhattacharyya, and K. Pal, "IoT-Based Applications in Healthcare Devices," 2021, Hindawi Limited. doi: 10.1155/2021/6632599.

[8] I. Ahmed and F. Lanonaca, "Recent Development in IoMT based Biomedical Measurement Systems: a Review."

[9] P. Mishra and G. Singh, "Internet of Medical Things Healthcare for Sustainable Smart Cities: Current Status and Future Prospects," Applied Sciences (Switzerland), vol. 13, no. 15, Aug. 2023, doi: 10.3390/app13158869.

[10] Y. A. Qadri, Zulqarnain, A. Nauman, A. Musaddiq, E. Garcia-Villegas, and S. W. Kim, "Preparing Wi-Fi 7 for Healthcare Internet-of-Things," Sensors, vol. 22, no. 16, Aug. 2022, doi: 10.3390/s22166209.

[11] T. Yaqoob, H. Abbas, and M. Atiquzzaman, "Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices-A Review," IEEE Communications Surveys and Tutorials, vol. 21, no. 4, pp. 3723–3768, Oct. 2019, doi: 10.1109/COMST.2019.2914094.

[12] T. Jabeen, H. Ashraf, and A. Ullah, "A survey on healthcare data security in wireless body area networks," J Ambient Intell Humaniz Comput, vol. 12, no. 10, pp. 9841–9854, Oct. 2021, doi: 10.1007/s12652-020-02728-y.

[13] P. Thippun, Y. Sasiwat, D. Buranapanichkit, A. Booranawong, N. Jindapetch, and H. Saito, "Implementation and experimental evaluation of dynamic capabilities in wireless body area networks: different setting parameters and environments," Journal of Engineering and Applied Science, vol. 70, no. 1, Dec. 2023, doi: 10.1186/s44147-022-00171-8.

[14] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," Jun. 01, 2015, Academic Press Inc. doi: 10.1016/j.jbi.2015.04.007.

[15] L. M. Tseng, P. F. Chen, and C. Y. Wen, "Design of Edge-IoMT Network Architecture with Weight-Based Scheduling," Sensors (Basel), vol. 23, no. 20, Oct. 2023, doi: 10.3390/s23208553.

[16] S. Zou, Y. Xu, H. Wang, Z. Li, S. Chen, and B. Hu, "A Survey on Secure Wireless Body Area Networks," 2017, Hindawi Limited. doi: 10.1155/2017/3721234.

[17] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure Medical Data Transmission Model for IoT-Based Healthcare Systems," IEEE Access, vol. 6, pp. 20596–20608, Mar. 2018, doi: 10.1109/ACCESS.2018.2817615.

[18] A. L. Martínez, M. G. Pérez, and A. Ruiz-Martínez, "A Comprehensive Review of the State-of-the-Art on Security and Privacy Issues in Healthcare," ACM Comput Surv, vol. 55, no. 12, Mar. 2023, doi: 10.1145/3571156.

[19] M. Papaioannou et al., "A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT)," Transactions on Emerging Telecommunications Technologies, vol. 33, no. 6, Jun. 2022, doi: 10.1002/ett.4049.

[20] M. S. Akhtar and T. Feng, "A Systemic Security and Privacy Review: Attacks and Prevention Mechanisms over IOT Layers," ICST Transactions on Security and Safety, vol. 8, no. 30, p. e5, Aug. 2022, doi: 10.4108/eetss.v8i30.590.

[21] A. Ahad et al., "A Comprehensive review on 5G-based Smart Healthcare Network Security: Taxonomy, Issues, Solutions and Future research directions," Jul. 01, 2023, Elsevier B.V. doi: 10.1016/j.array.2023.100290.

[22] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security," IEEE Internet Things J, vol. 8, no. 11, pp. 8707–8718, Jun. 2021, doi: 10.1109/JIOT.2020.3045653.

[23] M. Wazid, J. Singh, A. K. Das, S. Shetty, M. K. Khan, and J. J. P. C. Rodrigues, "ASCP-IoMT: AI-Enabled Lightweight Secure Communication Protocol for Internet of Medical Things," IEEE Access, vol. 10, pp. 57990–58004, 2022, doi: 10.1109/ACCESS.2022.3179418.

[24] P. K. Sahoo, S. R. Pattanaik, and S. L. Wu, "Design and analysis of a low latency deterministic network MAC for wireless sensor networks," Sensors (Switzerland), vol. 17, no. 10, Oct. 2017, doi: 10.3390/s17102185.
[25] V. Richert, B. Issac, and N. Israr, "Implementation of a modified wireless sensor network MAC protocol for critical environments," Wirel Commun Mob Comput, vol. 2017, 2017, doi: 10.1155/2017/2801204.
[26] M. Fotouhi, M. Bayat, A. K. Das, H. A. N. Far, S. M. Pournaghi, and M. A. Doostari, "A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT," Computer Networks, vol. 177, Aug. 2020, doi: 10.1016/j.comnet.2020.107333.
[27] T. Wan, L. Wang, W. Liao, and S. Yue, "A lightweight continuous authentication scheme for medical wireless body area networks," Peer Peer Netw Appl, 2021, doi: 10.1007/s12083-021-01190-7.
[28] W. Villegas-Ch, J. García-Ortiz, and I. Urbina-Camacho, "Framework for a Secure and Sustainable Internet of Medical Things, Requirements, Design Challenges, and Future Trends," Applied Sciences (Switzerland), vol. 13, no. 11, Jun. 2023, doi: 10.3390/app13116634.
[29] I. Ullah, M. A. Khan, A. M. Abdullah, F. Noor, N. Innab, and C. M. Chen, "Enabling Secure Communication in Wireless Body Area Networks with Heterogeneous Authentication Scheme," Sensors, vol. 23, no. 3, Feb. 2023, doi: 10.3390/s23031121.
[30] M. H. Nasir, J. Arshad, and M. M. Khan, "Collaborative device-level botnet detection for internet of things," Comput Secur, vol. 129, Jun. 2023, doi: 10.1016/j.cose.2023.103172.
[31] J. O. Healthcare Engineering, "Retracted: Designing a Healthcare-Enabled Software-Defined Wireless Body Area Network Architecture for Secure Medical Data and Efficient Diagnosis," 2023, NLM (Medline). doi: 10.1155/2023/9805042.
[32] Minahil, M. F. Ayub, K. Mahmood, S. Kumari, and A. K. Sangaiah, "Lightweight authentication protocol for e-health clouds in IoT-based applications through 5G technology," Digital Communications and Networks, vol. 7, no. 2, pp. 235–244, May 2021, doi: 10.1016/j.dcan.2020.06.003.
[33] M. Azees, P. Vijayakumar, M. Karuppiah, and A. Nayyar, "An efficient anonymous authentication and confidentiality preservation schemes for secure communications in wireless body area networks," Wireless Networks, vol. 27, no. 3, pp. 2119–2130, Apr. 2021, doi: 10.1007/s11276-021-02560-y.
[34] L. Zheng, Z. Wang, and S. Tian, "Comparative study on electrocardiogram encryption using elliptic curves cryptography and data encryption standard for applications in Internet of medical things," in Concurrency and Computation: Practice and Experience, John Wiley and Sons Ltd, Apr. 2022. doi: 10.1002/cpe.5776.

Authors' Profiles

Dina Riyadh Ibrahim completed the B.S. in electrical engineering/ electronic from the University of Nineveh, College of Electronics Engineering, Department of Electronics, Iraq in 2006 and obtained a master's degree in electronics and communications engineering/electronics in 2011 from the University of Mosul. She has been working as a lecturer in the Communications Department, College of Electronics Engineering, Nineveh University since 2012.

Mohammed Younis Thanoun completed the B.S. in electrical engineering/ electronic and communication from the University of Mosul, Iraq, in 1991 and received the M.Sc. degree in electronic and communication in 2000 and Ph.D. in 2011 from Mosul University. He is interested in the field of computer networks and communication and he has published research papers in Deep Learning, SDN, machine learning algorithms and cybersecurity engineering He has been working as an assistant professor at the University of Mosul since 2021. He is a member of the computer networks lab in the Electrical Dept. / Engineering College.

How to cite this paper: Dina Riyadh Ibrahim, Mohammed Younis Thanoun, "IoMT Survey: Device, Architecture, Communication Protocols, Application and Security", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.14, No.6, pp. 68-80, 2024. DOI:10.5815/ijwmt.2024.06.05